Corporate Governance and the Insider Threat: Investigating the Impact of Management Teams on Data Breaches

Miloslava Plachkinova, PhD[1]
Kennesaw State University,
Kennesaw, GA, USA

Prachi Gala, PhD
Kennesaw State University
Kennesaw, GA, USA

ABSTRACT

Data breaches have been on the rise for the past decade and no industry has been spared. Trusted personnel within the organization poses a major challenge because of the potential to cause significant damage. Costs of data breaches are only going to rise in the future, so it is important to analyze the role of senior management in protecting their organizations. The current study addresses this cybersecurity threat by exploring the impact of management teams on data breaches in the US. More specifically, we examine one of the critical infrastructure sectors - communications. We focus on T-Mobile, because from 2009 to 2023 the company has been affected by twelve data breaches, caused by both malicious hackers and employees. We incorporate two kernel theories, signaling theory and upper echelon theory, to develop our research model, and understand whether management teams and attackers' intent have an impact on stock market returns.

Keywords: data breach, stock return, management teams, insider threat.

INTRODUCTION

Data breaches have been on the rise for the past decade and no industry has been spared. According to the 2024 IBM report[2], the global average cost of a data breach reached $4.88 million – a 10% increase over last year and the highest total ever. Trusted personnel within the organization poses a major challenge and, in spite of the recent advancements in deep learning algorithms (Yuan and Wu 2021), they still have the potential to cause significant damages. Costs

[1] Corresponding author. mplachki@kennesaw.edu +1 (470) 478-4302
[2] https://www.ibm.com/reports/data-breach, accessed on October 1, 2024.

of data breaches are only going to rise in the future (Neto et al. 2021), so it is important to analyze how organizations are affected by such threats and what is the role of senior management in protecting their organizations, especially in terms of understanding how corporate governance can be used as a tool to influence employee behavior and attitudes.

The motivation behind writing this research paper stems from the growing concern over data breaches and their detrimental impact on organizations and stakeholders. As cyber threats continue to evolve, the role of management teams in shaping corporate governance and mitigating risks has become a critical area of focus. This study seeks to explore the intersection of leadership practices, corporate governance, and the insider threat, with the aim of understanding how management decisions influence vulnerability to data breaches. By analyzing this relationship, the research hopes to provide insights into better governance strategies that can enhance data security and reduce the risk of internal breaches.

The current study addresses these issues by exploring in more detail the impact of management teams on data breaches in the US. More specifically, we examine one of the critical infrastructure sectors–communications–based on the criteria outlined by the Cybersecurity and Infrastructure Security Agency (CISA)[3]. We selected T-Mobile, one of the major US telecommunication companies, to test our proposed research model. The company has been affected by twelve data breaches from 2009 to 2023 (Reed 2023), caused by both internal and external threats. The goal of this study is to explore potential differences between these two types of attacks when it comes to stock returns, senior management profiles, and organizational structures of Fortune 500 companies. More specifically, we investigate the spillover effect of the T-Mobile breaches on their competitors within the telecommunications sector in the US. The

[3] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector, accessed on October 1, 2024.

research question guiding this study is: *"How do a firm's leadership roles and cybersecurity incidents influence the stock returns of its competitors through spillover effects?"* To answer it, we integrate theories of corporate governance and information security governance. As this is research in progress, next, we plan to utilize secondary data and to perform quantitative analysis to identify factors that can be used by companies in the future to mitigate security risks and financial and reputational damage resulting from attacks on their competitors. Our work raises awareness on a problem of growing importance, and we provide both practical implications and theoretical contributions.

BACKGROUND

Insider Threats

Information systems (IS) within organizations are exposed to a variety of security threats, many of which may originate from inside of an organization. Prior literature has identified the lack of a unified definition of the term "insider threat" (Homoliak et al. 2019). Typically, it refers to threats originating from people who have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organization (Theoharidou et al. 2005). Some of the most common attributes of insiders consist of logical or physical location, authorization, expected behavior, motivation, and trust (Kandias et al. 2010). Insider threats are further broken down into two larger categories – accidental and malicious. This study explores how both types of insider threats affect organizations and whether intent is perceived as a potential factor when exploring consequences of data breaches within the telecommunications sector.

Corporate Governance

Corporate governance is concerned with "processes, customs, policies, laws and institutions that directs the organizations and corporations in the way they act, administer and control their operations" (Khan, 2011, p. 1). Its purpose is to achieve the goals of the organization and to manage the relationships among the stakeholders including the board of directors and the shareholders. In the context of the insider threat, corporate governance is especially important as C-suite executives are the ones who set the tone for the entire organization and whose responsibility is to develop policies and ensure compliance with regulations (Trautman and Moeller 2020). Another main responsibility of the C-suite executives is to manage crises and ensure that their organizations can survive disruptive events such data breaches, ransomware attacks, and other cyber-related incidents (Haislip et al. 2021). Data breaches can have a significant effect on organizations, because they often entail a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed (Esayas 2015).

While C-suite roles and responsibilities may differ across companies, it is important to establish a solid understanding of the organizational structure to evaluate whether there is any relationship between corporate governance and insider threats that resulted in data breaches. According to Guadalupe et al. (2014), top management structures in large US firms have changed significantly since the mid-1980s as a result of firm diversification and information technology investments. New Chief Officer roles have also emerged as strategic responses to institutional complexity (Svejenova and Alvarez 2017). Specifically, when it comes to Chief Information Officers (CIOs), there is a perception that the poor CIOs are doomed to short job

tenures due to the speed of technology refreshment, in spite of the fact that they contribute to the success of the organization by successfully managing technology (Dawson et al. 2015). These factors motivated us to further study the interplay between corporate governance and insider threats.

THEORETICAL FOUNDATION

Signaling theory, introduced by Spence (1973), examines how firms use signals to communicate information about their products or services to consumers, competitors, and stakeholders. These signals act as indicators of qualities like product reliability or the firm's intentions, which are difficult to assess directly. In IS, signaling theory focuses on how organizations signal their IT capabilities, intentions, or reliability (Dimoka et al. 2012). Applications include investment decisions and cybersecurity. Investors assess IT investments based on signals like R&D spending or technology partnerships (Ndofor and Levitas 2004), while organizations signal cybersecurity commitment through investments and industry involvement (Casey et al. 2016).

Upper Echelon Theory, proposed by Hambrick and Mason (1984, argues that the traits, experiences, and values of top executives influence organizational strategies and outcomes. In IS, this theory suggests that top management's background and biases shape how organizations perceive and invest in IT (Hiebl 2014). It focuses on observable demographic traits of top teams to explain organizational outcomes (Finkelstein and Hambrick 1996), such as performance and strategic decisions like internationalization or mergers (Wang et al. 2016). However, little attention has been given to the C-suite's impact during data breaches. Upper Echelon Theory highlights how executives' risk perception and decision-making shape cybersecurity posture and

resilience (Herath and Rao 2009; Héroux and Fortin 2022; Ogbanufe et al. 2021). Understanding these factors is crucial for effective cybersecurity strategies.

RESEARCH MODEL

While prior studies have been conducted to investigate the impact of data breaches on stock market returns (Johnson et al. 2017), none of them has specifically differentiated the breaches using the intent of the attacker. Thus, based on the kernel theories we incorporated, we designed a research model to answer the question guiding this study (Fig. 1). We also developed four hypotheses to investigate each aspect of the model more specifically.

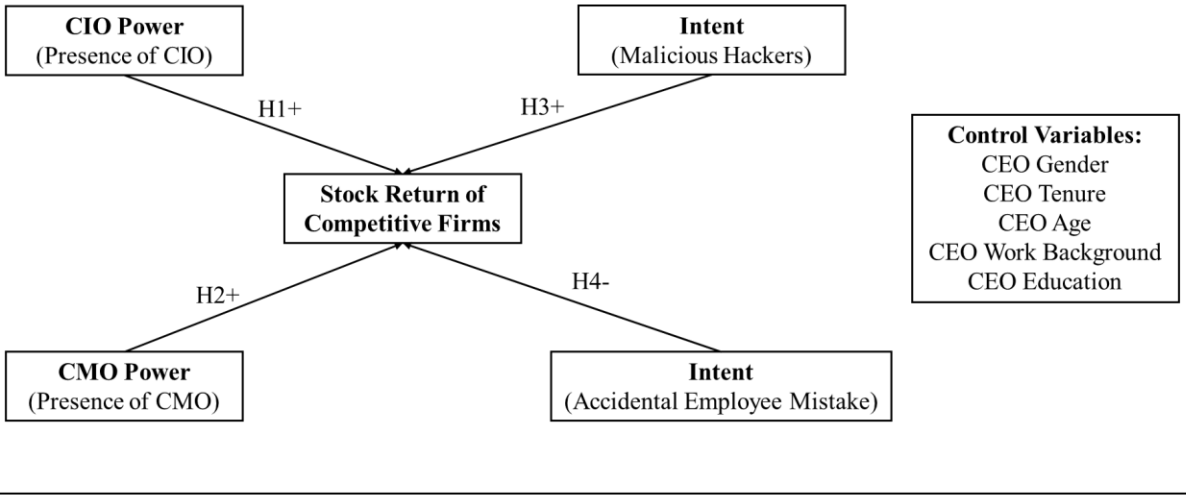

Figure 1. Proposed Research Model

H1: The presence of a Chief Information Officer (CIO) or a similar position will have a positive impact on the stock return of competitive firms not directly affected by the security breach.

Other studies have identified that such upper echelon positions add value to the firm performance (Xu et al. 2016) and have the potential to affect stock prices (Zhan et al. 2020). Thus, we expect to see that companies that have invested in building and supporting their IT capabilities would be more likely to avoid the negative consequences of data breaches.

H2: The presence of a Chief Marketing Officer (CMO) or a similar position will have a positive impact on the stock return of competitive firms not directly affected by the security breach.

CMO duties can also include proactively communicating with shareholders when a competitor has been affected by a security incident and explaining what the firm is doing to prevent any such attacks on its own systems and networks. Data breach announcements can affect customer behavior, brand loyalty, and trust (Kirk and Noguera 2019). Thus, we expect to see that strategic marketing efforts regarding cybersecurity issues are positively affecting stock returns.

H3: Malicious intent of hackers will have a positive impact on the stock return of competitive firms not directly affected by the security breach.

If hackers are taking advantage of firms, extorting them for money through ransomware, shareholders could be sympathetic to the victim (Butt et al. 2020). Thus, although the incident may have negative short-term financial consequences in terms of restoring systems and networks, we expect to see that a carefully crafted media campaign that demonstrates the firm got hacked despite its best efforts, can control the narrative in a more favorable light.

H4: Accidental employee mistake causing a data breach will have a negative impact on the stock return of competitive firms not directly affected by the security breach.

The rationale for this hypothesis is that organizations now are expected (and often legally mandated) to conduct regular cybersecurity training to their employees. While such training programs may not completely eliminate the threat, they have been proven effective in reducing it (Hu et al. 2021). Thus, if an employee mistakenly causes a data breach, it may be a lot more challenging to communicate such negligence to shareholders and create a positive narrative.

METHODOLOGY

To test the proposed model, we plan to incorporate secondary data ExecuComp, COMPUSTAT, and open-source intelligence to conduct quantitative analysis. We selected T-Mobile as a case study for this project since it has been affected by several data breaches caused both by malicious attackers outside of the organization as well as accidentally by employees of the company (Reed 2023). Since the attacks range from 2009 to 2023, there will be sufficient data to conduct the study and empirically test our model. To investigate how one event can impact the stock market returns of the companies in the same industry, we utilize the event study (Stäbler and Gala 2024). We will calculate the expected stock returns and compare it with the actual stock returns that happened because of the event, giving us the value of abnormal returns. We will utilize Fama French/Carhart four-factor model for the same (Fama et al. 1993). This abnormal stock return value will then serve as our dependent variable.

CONCLUSION

Data breaches have a much larger impact beyond just the organization directly affected by the attack. This spillover effect is important to investigate as it may help firms improve their crisis management efforts. We show that although a company may not be directly affected by a data breach, there could still be consequences for the entire industry. Thus, organizations need to prepare by expanding their marketing efforts and improving the overall security posture of the firm. This strategic alignment of resources can lead to building resilience and capability, sending a positive message to relevant stakeholders. Further, exploring how attacker motivation can potentially affect stock return is a novel concept that has not yet been investigated and our study is among the first to examine its impact on firm performance.

REFERENCES

Butt, U. J., Abbod, M. F., and Kumar, A. 2020. "Cyber Threat Ransomware and Marketing to Networked Consumers," in *Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer*. IGI Global, pp. 155-185.

Casey, W., Morales, J. A., Wright, E., Zhu, Q., and Mishra, B. 2016. "Compliance Signaling Games: Toward Modeling the Deterrence of Insider Threats," *Computational and Mathematical Organization Theory* (22), pp. 318-349.

Dawson, G. S., Ho, M.-W., and Kauffman, R. J. 2015. "How Are C-Suite Executives Different? A Comparative Empirical Study of the Survival of American Chief Information Officers," *Decision Support Systems* (74), pp. 88-101.

Dimoka, A., Hong, Y., and Pavlou, P. A. 2012. "On Product Uncertainty in Online Markets: Theory and Evidence," *MIS quarterly*), pp. 395-426.

Esayas, S. 2015. "The Role of Anonymisation and Pseudonymisation under the Eu Data Privacy Rules: Beyond the 'All or Nothing'approach," *European Journal of Law and Technology* (6:2).

Fama, E. F., French, K. R., Booth, D. G., and Sinquefield, R. 1993. "Differences in the Risks and Returns of Nyse and Nasd Stocks," *Financial Analysts Journal* (49:1), pp. 37-41.

Finkelstein, S., and Hambrick, D. C. 1996. *Strategic Leadership: Top Executives and Their Effects on Organizations*. Citeseer.

Guadalupe, M., Li, H., and Wulf, J. 2014. "Who Lives in the C-Suite? Organizational Structure and the Division of Labor in Top Management," *Management Science* (60:4), pp. 824-844.

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), pp. 318-334.

Hambrick, D. C., and Mason, P. A. 1984. "Upper Echelons: The Organization as a Reflection of Its Top Managers," *Academy of management review* (9:2), pp. 193-206.

Herath, T., and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Héroux, S., and Fortin, A. 2022. "Board of Directors' Attributes and Aspects of Cybersecurity Disclosure," *Journal of Management and Governance*), pp. 1-46.

Hiebl, M. R. 2014. "Upper Echelons Theory in Management Accounting and Control Research," *Journal of Management Control* (24), pp. 223-240.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., and Ochoa, M. 2019. "Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," *ACM Computing Surveys (CSUR)* (52:2), pp. 1-40.

Hu, S., Hsu, C., and Zhou, Z. 2021. "Security Education, Training, and Awareness Programs: Literature Review," *Journal of Computer Information Systems*), pp. 1-13.

Johnson, M., Kang, M. J., and Lawson, T. 2017. "Stock Price Reaction to Data Breaches," *Journal of Finance Issues* (16:2), pp. 1-13.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., and Gritzalis, D. 2010. "An Insider Threat Prediction Model," *International conference on trust, privacy and security in digital business*: Springer, pp. 26-37.

Khan, H. 2011. "A Literature Review of Corporate Governance," *International Conference on E-business, management and Economics*, pp. 1-5.

Kirk, G., and Noguera, J. 2019. "Strategic Marketing and Cybersecurity: The Case of Data Breaches," *Issues in Information Systems* (20:3).

Ndofor, H. A., and Levitas, E. 2004. "Signaling the Strategic Value of Knowledge," *Journal of Management* (30:5), pp. 685-702.

Neto, N. N., Madnick, S., Paula, A. M. G. D., and Borges, N. M. 2021. "Developing a Global Data Breach Database and the Challenges Encountered," *Journal of Data and Information Quality (JDIQ)* (13:1), pp. 1-33.

Ogbanufe, O., Kim, D. J., and Jones, M. C. 2021. "Informing Cybersecurity Strategic Commitment through Top Management Perceptions: The Role of Institutional Pressures," *Information & management* (58:7), p. 103507.

Reed, C. 2023. "T-Mobile Data Breaches: Full Timeline through 2023." from https://firewalltimes.com/t-mobile-data-breaches/

Spence, M. 1973. "Job Market Signalling," *Quarterly Journal of Economics* (87:3), pp. 355-374.

Stäbler, S., and Gala, P. 2024. "Breaking the News: How Does Ceo Media Coverage Influence Consumer and Investor Evaluations?," *Marketing Letters*), pp. 1-18.

Svejenova, S., and Alvarez, J. L. 2017. "Changing the C-Suite: New Chief Officer Roles as Strategic Responses to Institutional Complexity," in *New Themes in Institutional Analysis*. Edward Elgar Publishing, pp. 135-161.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of Iso17799," *Computers & Security* (24:6), pp. 472-484.

Trautman, L., and Moeller, M. 2020. "The Role of the Border and Border Policies in Efforts to Combat Human Trafficking: A Case Study of the Cascadia Region of the Us-Canada Border," *The Palgrave International Handbook of Human Trafficking*), pp. 985-999.

Wang, G., Holmes Jr, R. M., Oh, I. S., and Zhu, W. 2016. "Do Ceos Matter to Firm Strategic Actions and Firm Performance? A Meta-Analytic Investigation Based on Upper Echelons Theory," *Personnel Psychology* (69:4), pp. 775-862.

Xu, F., Zhan, H., Huang, W., Luo, X. R., and Xu, D. 2016. "The Value of Chief Data Officer Presence on Firm Performance," *Pacific Asia Conference on Information Systems, PACIS 2016-Proceedings*: AIS Electronic Library (AISeL), p. Paper 213.

Yuan, S., and Wu, X. 2021. "Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities," *Computers & Security* (104), p. 102221.

Zhan, X., Mu, Y., Nishant, R., and Singhal, V. R. 2020. "When Do Appointments of Chief Digital or Data Officers (Cdos) Affect Stock Prices?," *IEEE Transactions on Engineering Management* (69:4), pp. 1308-1321.