9-2024

# Strategic Cybersecurity Management: The Impact of Knowledge Resources and Capabilities on Data Breach Risk

Mohammad Mohsin
*University of North Carolina at Greensboro*, m_mohsin@uncg.edu

A.F. Salam
*University of North Carolina at Greensboro*, amsalam@uncg.edu

Moez Farokhnia Hamedani
*University of North Carolina Greensboro*, m_farokhnia@uncg.edu

**IRAIS**
Annual Conference on Information Systems

# Strategic Cybersecurity Management: The Impact of Knowledge Resources and Capabilities on Data Breach Risk

Mohammad Mohsin m_mohsin@uncg.edu; A F Salam amsalam@uncg.edu; Moez Farokhniahamedani m_farokhnia@uncg.edu

## Introduction

The unprecedented growth of cybercrime has led to a surge in data breaches, affecting hundreds of firms around the world. In 2023, 550 firms experienced data breaches (IBM 2024). The average cost of data breaches has been estimated to reach $4.45 million (IBM 2024), with indirect costs including decreased firm value, reputation, and competitive advantage (Foerderer and Schuetz 2022; Goel and Shawky 2009). This backdrop has encouraged researchers to explore the factors associated with data breach events and efficient cyber-defense strategies.

Studies suggest that data breach events are occurred by both IS/IT and non-IS/IT environments of a firm. While significant preventive factors within the former include IT security investment, IT modernization, and vulnerable disclosure, CSR (corporate social responsibilities), mergers and acquisitions, and financial disclosure have been identified as significant antecedents within the latter (Schlackl et al. 2022). Given that these factors seem to be dynamic and deeply rooted in organizational practices, firms often face “strategic balance dilemma”. To justify, on one hand, firms’ security practices, such as employee security trainings, and security awareness, were shown to curb the risk of security breaches(Kweon et al. 2021; Li et al. 2023). On the other hand, their social practices, such as corporate social responsibility, may often lead to the increased risk of security breaches (D’Arcy et al. 2020). This highlights the criticality of strategic cybersecurity risk management. Given the growing cybersecurity talent gap and the increasing demand for cyber workforce, 93% of firms plan to outsource portions of their cybersecurity risk management to specialized service providers in the next two years (Newswire 2023). However, this strategy introduces new risks, as the rise of generative AI lowers the barrier for low-skilled adversaries to launch sophisticated attacks (CrowdStrike 2024). While outsourcing can offer benefits, it also poses security risks (Almutairi and Riddle 2018).

Motivated by these developments, we consider two organizational strategic factors—(1) cybersecurity knowledge resources and (2) cybersecurity capabilities—in the context of data breach risk. We consider both external and external facets in the former, and proactive, protective as well as AI-based aspects in the latter. Cybersecurity knowledge resources are referred to, in this study, organizational cybersecurity personnel and their strategic management with respect to cybersecurity technologies. Likewise, cybersecurity capabilities are referred to a dynamic capability of the firm to strategically prevent cyber threats. Our conceptualization of these factors is motivated by two seminal works in organizational knowledge (Spender and Grant 1996) and dynamic capability (Teece et al. 1997), respectively. Therefore, by drawing on the lens of organizational knowledge-based view and dynamic capability, our objective is to empirically investigate the impact of cybersecurity knowledge resources and capabilities on the likelihood of data breaches.

The importance of this study is three-fold. First, despite the emphasis on the potential of cybersecurity capabilities to mitigate cyber threats (Naseer et al. 2018), there is limited empirical evidence providing insights into organizational strategical choices between preventive, proactive and AI-based cybersecurity capabilities. Second, the exploration of cyberattacks in recent years have motivated many firms for security outsourcing. As concern about the risk in security outsourcing persists (Benaroch 2020), studies investigating the impact of blending cybersecurity knowledge resources (both external and internal) remain limited. Third, we aim to provide managerial strategic insights into how cybersecurity knowledge resources and capabilities impact the likelihood of data breaches. As we highlighted earlier, this strategic movement is critical in reducing data breach risk.

## Methodology and Conclusion

Our sample construction will include several sources of data. To operationalize the outcome variable, we aim to use data from Privacy Rights Clearinghouse (PRC) (D'Arcy et al. 2020). This dataset has been used in the breach literature measure data breach risk. Our second source encompasses a unique dataset from an online platform that has a great repository of data, including cybersecurity employees, measures, applications, and IT. We aim operationalize all explanatory variables from this dataset. For controls, we aim to use data from S&P 500. To test our formulated hypotheses, we aim to use regression models, specifically an ordinary least squares (OLS) panel fixed effects model. We expect that our study will provide evidence that cybersecurity knowledge resources and capabilities are negatively associated with data breach risk. Furthermore, firms with higher internal cybersecurity resources than external resources will experience fewer data breaches. Likewise, firms with higher proactive cybersecurity capability than preventive capability will observe fewer data breaches.

## References

IBM. 2024. "Cost of a Data Breach Report," p. 2.

Foerderer, J., and Schuetz, S. W. 2022. "Data Breach Announcements and Stock Market Reactions: A Matter of Timing?," *Management Science* (68:10), pp. 7298-7322.

Goel, S., and Shawky, H. A. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information & Management* (46:7), pp. 404-410.

Kweon, E., Lee, H., Chai, S., and Yoo, K. 2021. "The Utility of Information Security Training and Education on Cybersecurity Incidents: An Empirical Evidence," *Information Systems Frontiers* (23), pp. 361-373.

Li, W. W., Leung, A. C. M., and Yue, W. T. 2023. "Where Is It in Information Security? The Interrelationship among It Investment, Security Awareness, and Data Breaches," *MIS Quarterly* (47:1), pp. 317-342.

Schlackl, F., Link, N., and Hoehle, H. 2022. "Antecedents and Consequences of Data Breaches: A Systematic Review," *Information & Management* (59:4), p. 103638.

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), pp. 1200-1223.

Benaroch, M. 2020. "Cybersecurity Risk in It Outsourcing—Challenges and Emerging Realities," *Information systems outsourcing: The era of digital transformation*), pp. 313-334.