6-14-2024

Examining The Factors Influencing Management Discretion On The Reporting Of Cybersecurity Incidents

Ahmad Jumah
University of Illinois Springfield, jumah@uis.edu

EXAMINING THE FACTORS INFLUENCING MANAGEMENT DISCRETION ON THE REPORTING OF CYBERSECURITY INCIDENTS

TREO Paper

Ahmad H. Juma'h

University of Illinois Springfield, USA

Abstract

This study investigates the factors affecting the timely reporting of data breaches by management and its subsequent impact on a company's financial performance. It examines how the rapidity of reporting relates to management's assessment of breach materiality, offering insights for future inquiries and assisting executives in considering disclosure variables. By exploring management discretion in breach disclosure, the research investigates the managerial decisions regarding timely reporting, addressing crucial inquiries concerning disclosure motivations and their effects on company performance. Previous research emphasizes the importance of considering breach attributes, including the volume and sensitivity of compromised data, in assessing materiality. Our study highlights the important role of timely and transparent communication post-breach, underscoring its influence on stakeholders' decisions and its potential to alleviate adverse consequences such as reputational damage and regulatory penalties.

Keywords: Cybersecurity incidents, Materiality, Reporting, SEC guidance.

1 Introduction

The focus on the financial implications of data breaches in the accounting and auditing fields derived from their increasing prevalence across sectors and their financial implications. Such breaches affect accounting methods, corporate disclosures, and overall business outcomes, necessitating continuous risk assessments. Accountants play a critical role in managing potential loss contingencies, disclosing risks, and addressing costs such as legal fees and customer notifications. Regulatory bodies like the SEC emphasize the importance of timely and transparent breach disclosures to investors. By understanding and addressing the financial implications of data breaches, accounting professionals can sustain integrity and transparency, assisting organizations manage and minimize the effects of cybersecurity incidents' consequences while maintaining stakeholder confidence and resilience (Cohn, 2022).

Data breach disclosure presents several challenges that impact stakeholders. Campbell et al. (2003) emphasized the financial implications of breaches involving sensitive data, often causing adverse reactions in the stock market. Jenkins et al. (2014) found that visual representations in breach notifications positively influence public perception, while apology letters have minimal impact on reputation. These insights highlight the critical role of strategic communication in mitigating breach consequences. Mossburg (2015) stressed the rising frequency of cyber-attacks, urging initiative-taking resource allocation for such incidents. Integrating these perspectives indicates the complexity of addressing data breaches and the need for comprehensive strategies. Furthermore, prior research suggests minimal consumer response to breach notifications, contrasting with negative market reactions

(Gwebu et al., 2018). Richardson et al. (2019) propose that breaches may increase in frequency with limited financial repercussions, prompting questions about the attention given to breach disclosure within the accounting profession.

This study investigates the factors influencing timely reporting of data breaches by management and its subsequent impact on a company's financial performance. It examines how prompt reporting reflects management's consideration of breach materiality, aiming to provide insights for future research and assist executives in understanding disclosure variables. By analyzing management discretion in breach disclosure, the study explores how managerial decisions influence reporting in a timely manner, addressing questions on disclosure motivation and the impact on company performance. Prior research highlights the importance of considering breach characteristics and the volume and sensitivity of compromised data in assessing materiality. Our study highlights the significance of timely and transparent communication post-breach, stressing its influence on stakeholders' decisions and mitigating negative impacts like reputational harm and regulatory penalties.

2 Theoretical background

Data breach disclosure involves several implications on stakeholders, as evidenced by research highlighting financial effects and the role of strategic communication in managing consequences. Campbell et al. (2003) emphasized negative stock market reactions to breaches involving sensitive data, while Jenkins et al. (2014) found that visual representations positively influence public perception, contrasting with apology letters' limited impact on reputation. Mossburg (2015) urged initiative-taking resource allocation to address the increasing frequency of cyber-attacks, particularly concerning consumer information. Integrating these insights emphasizes the complexity of breach management. Richardson et al. (2019) suggest a potential rise in breach occurrences with varied financial consequences, raising questions about the accounting profession's focus on breach disclosure. Cheng and Walton (2019) explored investor judgments, finding third-party disclosures favorably perceived over delayed disclosures by breached organizations, impacting market performance and regulatory discourse. Gordon et al. (2011) noted adverse stock price effects from breaches affecting confidentiality, availability, and integrity, while Juma'h and Alnsour's (2020, 2021) highlighted broader economic implications extending to non-breached firms.

Despite efforts to enhance disclosure practices, concerns persist regarding their effectiveness. According to Amir et al. (2018), there are modest increases in disclosure rates following SEC cybersecurity guidance but inconclusive evidence on market reactions, questioning the adequacy of self-disclosure by breached firms and advocating for mandatory notification guidance to address confusion stemming from state-level regulations. Ogle's (2019) investigation revealed weak reporting procedures' negative impacts on investor confidence and consumer trust, calling for regulatory reform. Consequently, the SEC released mandatory rules in July 2023 for public companies to report data breach incidents. This paper aims to contribute to existing literature by examining a broader sample of breaches to assess the impact of updated SEC guidance and exploring the relationship between breach materiality and disclosure timing. Financial reports play a crucial role in evaluating company performance and often contain discretionary disclosures about breaches and associated risks. Understanding the dynamics of data breach disclosure is crucial for regulatory frameworks and organizational practices to mitigate risks effectively.

3 Methods

Employing panel data methodology to analyze the relationship between data breaches and company performance, this study utilized secondary data from online databases like PrivacyRights.org and InformationIsBeautiful.net. PrivacyRights.org served as the primary data source, housing over 10,000 events since 2005, while InformationIsBeautiful.net validated data and identified major breaches. Google Search was used to validate announcement content in cases of discrepancies. The study included companies with financial reporting before and after data breach announcements, identifying 950 breach

events from 450 companies reporting required financial data yearly between 2005 and 2023. Leveraging comprehensive datasets and rigorous analytical techniques, this methodology offers a robust framework for examining the financial implications of data breaches on publicly traded companies. Financial variables were obtained from Mergent Online by the FTSE Russell database, focusing on public firms traded in US stock markets that announced breaches and are obligated to report to the SEC within four days using 8-k reports. The study's data, accessible through the EDGAR database, encompasses breach type, affected records, breach date, industry type, and public trading status, with financial variable definitions.

We expect to complete sections related to results, discussion, conclusions, limitations, and implications.

References

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies, 23, 1177-1206.

Campbell, K, Gordon, L., Loeb, M, and Zhou, L. (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11. IOS Press

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? Journal of Information Systems, 33(3), 163-182.

Cohn, M. (2022). SEC Urges Companies to Disclose More About Data Breaches. *Accounting Today*. Retrieved from https://www.accountingtoday.com/news/sec-urges-companies-to-disclose-more-about-data-breaches.

Gordon, L, Loeb, M, & Zhou, L. (2011) The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security 19. IOS Press.

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), pp. 683-714.

Jenkins, A., Anandarajan, M and D'Ovidio, R. (2014) 'All that Glitters is not Gold': The Role of Impression Management in Data Breach Notification. *Western Journal of Communication*. 8 (3), pp. 337-357.

Juma'h, A. H., & Alnsour, Y. (2019) The effect of data breaches on company performance. International Journal of Accounting & Information Management.

Juma'h, A. H., & Alnsour, Y. (2021) How Do Investor Perceive the Materiality of Data Security Incidents. Journal of Global Information Management. Volume 29, Issue 6.

Mossburg, E. (2015). A deeper look at the financial impact of cyber attacks. *Financial Executive*, 31(3), pp. 77-80.

Ogle, J. (2019) Identities Lost: Enactind Federal Law Mandating Disclosure & Notice After a Data Security Breach. Arkansas Law Review. Volume 72 Issue 1, p221-243.

Richardson, V., Smith, R., & Watson, M. (2019) Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*. 33(3), pp. 227-265.