

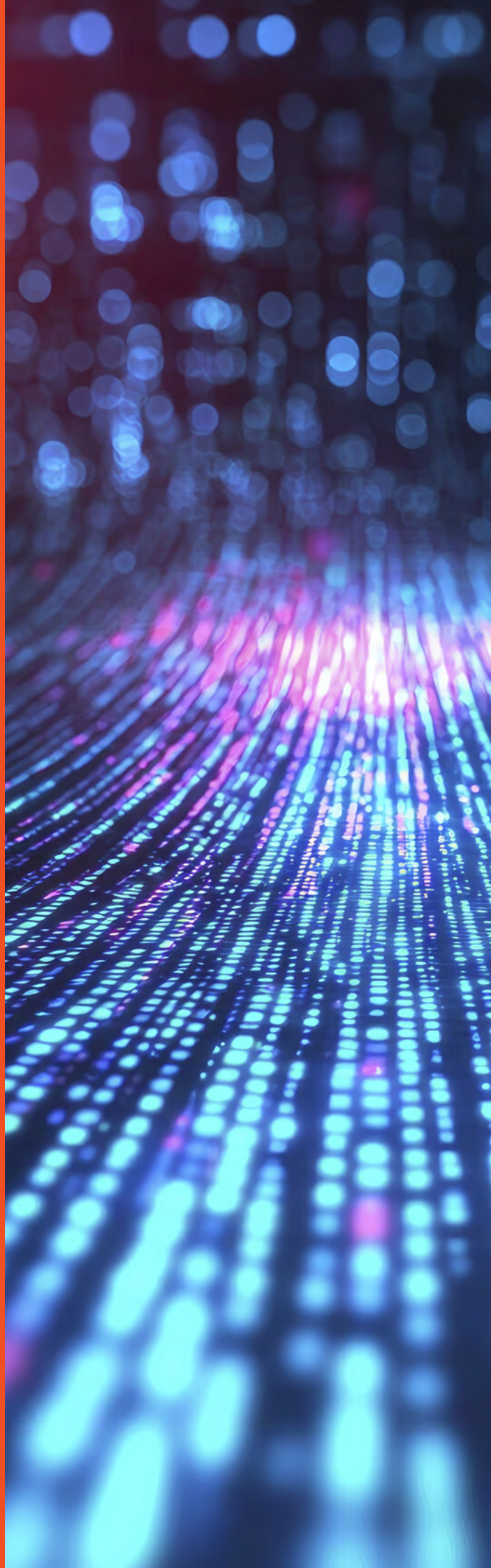


THE UNIVERSITY OF
SYDNEY

The University of Sydney Accounting Foundation

2023 Engaged Research Grant Scheme
Executive Summary

Exploring the Materiality of Data Breach Disclosures on the Australian Stock Exchange



Contents

Exploring the Materiality of Data Breach Disclosures on the Australian Stock Exchange	02
Key conclusions	02
Abstract	02
Introduction	03
Objectives	03
Research method	03
Main findings and implications for practice	04
Limited disclosures	04
Share price impacts	04
Costs	04
Announcement paradox	04
Materiality issues	04
Conclusions	06
References and further reading	07
Acknowledgments	09

We recognise and pay respect to the Elders and communities – past, present, and emerging – of the lands that the University of Sydney's campuses stand on. For thousands of years they have shared and exchanged knowledges across innumerable generations for the benefit of all.

Exploring the Materiality of Data Breach Disclosures on the Australian Stock Exchange

Key conclusions

The study reveals a significant lack of data breach disclosures on the ASX, with only a limited number of incidents announced from 2018–2021 despite over 3,776 breaches reported to the Office of the Australian Information Commissioner (OAIC) during the same period. We highlight a massive under-disclosure gap that has widened over time. Disclosures often lack detail, and materiality judgments are subjective and poorly justified, leading to delays in disclosure and increased contagion risks. After further study of significant breach announcements, we identify an “announcement paradox” and show that breaches become material over time as stakeholders react, amplifying costs. Recommendations include developing “likely-market-effect models” (e.g., inspired by FAIR-MAM) for estimating share price impacts to improve transparency, governance, and decision-making on disclosures, with global applicability.

Abstract

This study examines Australian Stock Exchange (ASX) data breach announcements to provide insights into the extent and nature of data breach disclosures, as well as the costs, particularly to stakeholder relationships. Using a dataset of all data breach-related announcements on the ASX, we identify a lack of data breach disclosure and, where disclosures are made, a notable absence of detail. To examine how the concept of materiality is applied, given its role as a threshold for disclosure to stock markets globally, we provide an in-depth examination of the case of Landmark White (LMW), the only company to disclose a material impact from its data breaches to the ASX. We identify an announcement paradox, where the data breach at LMW became material over time as stakeholders reacted to the announcements, pointing to a contagion effect. We recommend the creation of likely-market-effect models, which allow companies to calculate the likely share price impact of a data breach and use this in their decision to disclose. This approach represents a simple first step in reconceptualizing continuous disclosure regimes for the digital age, aimed at enhancing the transparency and reporting of cyber incidents to stock markets globally.



Introduction

Globally, data breaches are on the rise, prompting increasing scrutiny from capital markets and regulators regarding their impact on firm value and stakeholder risks (Verizon, 2021; PwC, 2020). This study draws on Australian data to offer insights into market-relevant disclosures amid this global trend, providing internationally applicable recommendations despite its empirical focus on Australia. Australian companies face mounting pressure to safeguard customer data under regulatory frameworks such as the Notifiable Data Breaches (NDB) scheme, APRA Prudential Standard CPS 234 (APRA, 2019), and ASX continuous disclosure obligations (ASX, 2024). Empirical evidence consistently shows negative effects on market value and stock performance from data breaches (Garg et al., 2003; Ettredge and Richardson, 2003; Cavusoglu et al., 2004; Acquisti et al., 2006). Recent studies highlight how timely managerial responses, such as apologies, can mitigate adverse reactions (Foerderer and Schuetz, 2022; Nikkhah and Grover, 2022; Masuch et al., 2022), yet research on actual disclosure practices remains limited, leading to gaps in understanding the nature and extent of breaches (Gibson and Harfield, 2021; Neto et al., 2021; Thomas et al., 2022) and challenges in determining materiality under stock market guidelines that rely on managerial judgment. This paper investigates the actions and impacts of data breach announcements, aiming to provide insights into the extent, nature, and costs of disclosures (especially to stakeholder relationships) while addressing global challenges through an ASX focus. It extends the literature by examining the application of materiality as a disclosure threshold, identifying gaps in disclosure practices and levels of detail, and emphasising the “announcement paradox”, where financial impacts emerge over time. These issues are underscored by the scale of over 3,776 OAIC-reported breaches between 2018 and 2021 compared to the limited disclosures observed on the ASX.

Objectives

- To examine the extent and nature of data breach disclosures on the ASX.
- To identify the costs of data breaches, particularly the impacts on stakeholder relationships.
- To explore how materiality is applied as a disclosure threshold.
- To analyse gaps in disclosure practices and levels of detail.
- To investigate the “announcement paradox” where breaches become material over time due to stakeholder reactions.
- To recommend improvements, such as a likely-market-effect model, to enhance transparency in global continuous disclosure regimes.

Research method

Our mixed methods study employs both quantitative and qualitative research approaches in two phases. The initial phase involves quantitative data collection and analysis to provide a broad understanding of the limited number of breach events announced by entities listed on the ASX during the period between 1 January 2018 and 31 December 2021. A key focus was to highlight the under-disclosure relative to the vastly larger sample of over 3,776 OAIC-reported breaches during the same period. A total of 20 breach events were identified, of which only 11 were reported in the entities’ annual reports. The second phase takes a qualitative approach (Teddlie and Tashakkori, 2009) to examine the announcements, reporting, and share price changes of companies experiencing data breaches.

Our in-depth examination of these cases aimed to understand the tension within the concept of materiality, where the preparer determines the significance of information for the recipient. This often leads to delays in disclosure until the estimated impact of a data breach is understood, creating the announcement paradox inherent in this materiality threshold. Moreover, we examined the unique contagion risk associated with data breaches, which affects stakeholders’ perceptions of the company and prompts defensive actions.

Main findings and implications for practice

Limited disclosures

Only 20 breach events were disclosed on the ASX compared to over 3,776 breaches reported to the OAIC between 2018 and 2021, with minimal detail in single announcements, more in multiple announcements, strongly emphasising the massive scale of under-reported breaches in the broader sample.

Share price impacts

Minor for single announcements (around 2-5% declines, quick recovery); severe for multiple announcements (11-44% drops, prolonged).

Costs

Direct (e.g. recovery/remediation); indirect (e.g. reputational harm and financial losses, including in the LMW case \$5-6M lost revenue, \$12.284M impairments, and \$15.148M net losses in 2019).

Announcement paradox

Disclosures create contagion risk, as stakeholders such as banks may suspend lending relationships or take defensive actions.

Materiality issues

Subjective judgments delay disclosures; breaches become material post-announcement due to stakeholder reactions.





Conclusions

Implications

Companies should adopt likely-market-effect models to estimate impacts, enhancing governance and transparency. Regulators and industry could collaborate on public models to foster a proactive disclosure culture, reducing associated risks in the digital age. Our research is globally relevant for markets like NYSE, Nasdaq, LSE, EU.

References and further reading

- Acquisti, A., A. Friedman, and R. Telang (2006), 'Is There a Cost to Privacy Breaches? An Event Study', ICIS Proceedings, 94.
- Australian Prudential Regulation Authority (APRA) (2019), Prudential Standard CPS 234 Information Security, retrieved from https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.
- Australian Securities Exchange (2024), ASX Listing Rules. Guidance Note 8. Australian Securities Exchange Continuous Disclosure: Listing Rules 3.1 – 3.1B, retrieved from <https://www.asx.com.au/content/dam/asx/rules-guidance-notes-waivers/asx-listing-rules/guidance-notes/gn08-continuous-disclosure.pdf>.
- Ettredge, M. L. and V. J. Richardson (2003), 'Information Transfer Among Internet Firms: The Case of Hacker Attacks', Journal of Information Systems, Vol. 17, pp. 71–82.
- Foerderer, J. and S. W. Schuetz (2022), 'Data Breach Announcements and Stock Market Reactions: A Matter of Timing?', Management Science, Vol. 68, pp. 7298–322.
- Cavusoglu, H., B. K. Mishra, and S. Raghunathan (2004), 'The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers', International Journal of Electronic Commerce, Vol. 9, pp. 70–104.
- Garg, A., J. Curtis, and H. Halper (2003), 'Quantifying the Financial Impact of IT Security Breaches', Information Management & Computer Security, Vol. 11, pp. 74–83.
- Gibson, D. and C. Harfield (2021), 'Contradictions and Inconsistencies in Australia's Mandatory Data Breach Notification Laws', The Computer Law and Security Report, Vol. 42, 105600.
- Masuch, K., M. Greve, S. Trang, and L. M. Kolbe (2022), 'Apologize or Justify? Examining the Impact of Data Breach Response Actions on Stock Value of Affected Companies', Computers & Security, Vol. 112, 102502.
- Neto, N. N., S. Madnick, A. M. G. D. Paula, and N. M. Borges (2021), 'Developing a Global Data Breach Database and the Challenges Encountered', ACM Journal of Data and Information Quality, Vol. 13, pp. 1–33.
- Nikkhah, H. R. and V. Grover (2022), 'An Empirical Investigation of Company Response to Data Breaches', MIS Quarterly, Vol. 46, pp. 2163–96.
- PwC (2020), 23rd Global CEO Survey, retrieved 3 October 2023 from <https://www.pwc.com/gx/en/ceosurvey/2020/reports/pwc-23rd-global-ceo-survey.pdf>.
- Teddlie, C. and A. Tashakkori (2009), Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences, Sage, Thousand Oaks.
- Thomas, L., I. Gondal, T. Oseni, and S. A. Firmin (2022), 'A Framework for Data Privacy and Security Accountability in Data Breach Communications', Computers & Security, Vol. 116, 102657.
- Verizon (2021), 2021 Data Breach Investigations Report, retrieved 26 September 2023 from <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>.



Acknowledgments

The author(s) would like to thank
The University of Sydney Accounting
Foundation for funding this project.

Author(s), Author Affiliation, Author email address

Jane Andrew
Discipline of Accounting, Governance and Regulation,
The University of Sydney Business School,
The University of Sydney
jane.andrew@sydney.edu.au

Max Baker
Discipline of Accounting, Governance and Regulation,
The University of Sydney Business School,
The University of Sydney
max.baker@sydney.edu.au

Monique Sheehan
Discipline of Accounting, Governance and Regulation,
The University of Sydney Business School,
The University of Sydney
monique.sheehan@sydney.edu.au

Xiaojiao Wang
Discipline of Accounting, Governance and Regulation,
The University of Sydney Business School,
The University of Sydney
jo.wang@sydney.edu.au



If you want to collaborate with The University of Sydney Accounting Foundation on an engaged research project, please contact:
business.accountingfoundation@sydney.edu.au

For more information on what we do, please visit:
[sydney.edu.au/business/our-research/research-areas/
accounting-governance-and-regulation/
the-accounting-foundation](https://sydney.edu.au/business/our-research/research-areas/accounting-governance-and-regulation/the-accounting-foundation)