

**The Informativeness of Cybersecurity-Related Disclosures:**  
**Evidence from Australia and China**

Ruiyu Li

A research component submitted to Auckland University of Technology in partial fulfilment  
of the requirements for the degree of Master of Business

2026

School of Business, Economics and Law

Auckland University of Technology

## Abstract

Cybersecurity risk has become an important corporate reporting and capital-market issue as regulators increasingly expect firms to disclose cyber-related risks, governance, and risk management. However, it remains unclear whether these disclosures are useful for investment decisions or primarily reflect compliance with formal reporting requirements. Prior research has rarely examined cybersecurity disclosure informativeness in annual reports across distinct domestic regulatory regimes. This study addresses this gap by comparing Australia and China and examining whether disclosure informativeness is associated with the cost of equity. The study uses 600 firm-year observations from 100 Australian and 100 Chinese firms covering FY2022–FY2024 and develops a codebook-based Cybersecurity-Related Disclosure Score capturing specificity, relevance, and usefulness. First, Australian firms provide significantly more informative cybersecurity disclosures than Chinese firms across the aggregate score, all three dimensions, and most individual indicators, with the largest differences in specific threat identification and business consequence disclosure. Second, the aggregate CSRDS score and the three dimension-level scores are not significantly associated with the cost of equity, including after industry adjustment. At the indicator level, business-consequence disclosure provides supplementary evidence of a negative association in the CAPM joint-indicator model and remains statistically significant after the primary Holm multiple-testing adjustment; however, this adjusted inference is not uniform across alternative indicator specifications or the LSEG financing-cost outcome. Third, formal interaction tests show that neither the aggregate CSRDS association nor the business consequence disclosure association differs significantly between Australia and China. These findings suggest that institutional context is more clearly reflected in disclosure production than in cross-country variation in capital-market consequences. They also highlight the importance of distinguishing specific disclosure content from aggregate disclosure indices when assessing cost-of-equity associations in cybersecurity reporting.

## Keywords

Cybersecurity disclosure; Disclosure informativeness; Cost of equity; Institutional theory; Cross-country comparison; China; Australia.

## Table of Contents

|                                                         |     |
|---------------------------------------------------------|-----|
| Abstract                                                | 1   |
| Table of Contents                                       | 2   |
| List of Figures                                         | 3   |
| List of Tables                                          | 4   |
| Attestation of Authorship                               | 6   |
| AI Declaration Form                                     | 7   |
| Chapter 1. Introduction                                 | 8   |
| Chapter 2. Literature Review and Hypothesis Development | 22  |
| Chapter 3. Methodology and Data Collection              | 59  |
| Chapter 4. Results                                      | 81  |
| Chapter 5. Discussion and Implications                  | 114 |
| Chapter 6. Conclusion, Limitations, and Future Research | 126 |
| References                                              | 130 |
| Appendices                                              | 147 |

## **List of Figures**

|                                                               |    |
|---------------------------------------------------------------|----|
| Figure 4.1 Mean CSRDS Score by Country, FY2022-FY2024         | 89 |
| Figure 4.2 Indicator-Level Coefficients on the Cost of Equity | 99 |

## List of Tables

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| Table 2.1 Institutional Comparison of Disclosure Orientation in China and Australia   | 37  |
| Table 2.2 Mechanisms Linking Disclosure Informativeness to the Cost of Equity         | 49  |
| Table 2.3 Summary of Institutional Channels and Predicted Effects                     | 58  |
| Table 3.1 Sample Construction, Screening, and Replacement Process                     | 63  |
| Table 3.2 The CSRDS Codebook: Nine Indicators × Three-Level Ordinal Scale             | 66  |
| Table 3.3 Post-Refinement Validation Sample and Machine-Human Reliability             | 72  |
| Table 4.1 Descriptive Statistics                                                      | 83  |
| Table 4.2 Breakdown of Zero-Score CSRDS Observations                                  | 85  |
| Table 4.3 Pearson Correlation Matrix for the Main CoE Regression Variables            | 87  |
| Table 4.4 Mean CSRDS and Positive Score Incidence by Country and Fiscal Year          | 88  |
| Table 4.5 Cross-Country Comparison of Aggregate and Dimension-Level CSRDS Scores      | 90  |
| Table 4.6 Cross-Country Comparison of Indicator-Level CSRDS Scores                    | 91  |
| Table 4.7 Firm-Clustered H1 Country-Difference Regression Results                     | 93  |
| Table 4.8 H2 Cost of Equity Regressions for Aggregate CSRDS and CSRDS Dimensions      | 95  |
| Table 4.9 Joint Indicator Model of CSRDS and Cost of Equity                           | 98  |
| Table 4.10 H3 CoE Interaction Regression Results                                      | 101 |
| Table 4.11 Selected Robustness and Sensitivity Results                                | 104 |
| Table 4.12 Additional H1 Robustness Test with Broad Sector Fixed Effects              | 106 |
| Table 4.13 Industry fixed-effects robustness results                                  | 108 |
| Table 4.14 Holm-adjusted results for the indicator-level analyses                     | 111 |
| Table 3A.1 Industry Composition of the Original Eligible Pool and Final Locked Sample | 147 |
| Table 3A.2 Final Sample Firms by Country and Industry                                 | 148 |
| Table 3B.1 CSRDS Indicators and Definitions                                           | 158 |
| Table 3B.2 CSRDS Scoring Criteria                                                     | 160 |
| Table 3B.3 Active Bilingual Keyword Dictionary by Indicator                           | 163 |
| Table 3C.1 Indicator-Level Machine-Human Reliability for CSRDS Scoring                | 165 |
| Table 3C.2 Country-Specific Validation Reliability and Confidence Intervals           | 166 |
| Table 3C.3 Documented Indicator-Level Corrections in the Post-Refinement Validation   | 167 |
| Table 3D.1 Definitions and Measurement of Regression Variables                        | 168 |
| Table 4A.1 CAPM R2-Only Model                                                         | 169 |
| Table 4A.2 H2 Single-Indicator Screening Regressions                                  | 170 |
| Table 4B.1 CAPM Country-Subsample Regression Results for H3 Supplementary Analysis    | 171 |
| Table 4C.1 Alternative Financing Cost Robustness Using LSEG StarMine WACC             | 172 |

|                                                                           |     |
|---------------------------------------------------------------------------|-----|
| Table 4C.2 Winsorised CAPM Robustness Models                              | 173 |
| Table 4C.3 Positive CSRDS Indicator and Positive CSRDS Subsample Analyses | 173 |
| Table 4C.4 Governance-Control Robustness Models                           | 174 |
| Table 4D.1 Variance Inflation Factors for Final Regression Models         | 176 |

## **Attestation of Authorship**

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

**Signature:** 

**Full name:** Ruiyu Li

**Date:** 28/07/2026

## AI Declaration Form

|                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Specify the chapter number(s) in your research proposal/research component where AI was used.</i>                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Chapter number(s):</b>                                                                                                                     | Chapters 1-6, reference list and selected appendices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <i>Briefly explain why the AI tool was used (e.g., idea generation, summarization, data analysis, image creation, etc.).</i>                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Purpose of AI Use:</b>                                                                                                                     | AI was used to support language refinement, academic style improvement, structural feedback, clarification of methodological explanations, reference-list checking, appendix organisation, table-formatting guidance, and interpretation support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <i>Clearly state the AI tools used.</i>                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>AI Tool(s) Used:</b>                                                                                                                       | ChatGPT, Gemini                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <i>Prompts or queries entered into the AI tool (only the instructive portion of the prompt is required). Include all relevant variations.</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Prompts Used:</b>                                                                                                                          | <p>Please review this thesis section for academic clarity, logical flow, and consistency with accounting journal style.</p> <p>Please suggest how to organise appendix materials in an APA 7th/accounting journal table style.</p> <p>Please check whether the in-text citations correspond to entries in the reference list and whether the references follow APA 7th style.</p>                                                                                                                                                                                                                                                                                                                                                  |
| <i>A summary or description of the AI-generated output. (Optional: attach output in an appendix.)</i>                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Output Received:</b>                                                                                                                       | Language-editing suggestions, structural recommendations, consistency checks, table and appendix formatting guidance, and interpretive feedback on the empirical findings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <i>Describe how the AI output was used, edited, or transformed.</i>                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Post-AI Processing Methods:</b>                                                                                                            | I carefully reviewed all AI-generated suggestions and selectively incorporated those that I believed would genuinely improve my research. Every substantive decision, including research design and data collection, as well as coding, statistical analysis, interpretation of results, and final conclusions was made independently by me. Before incorporating any AI-generated suggestions, I cross-checked it against my thesis data, my supervisors' feedback, primary sources, the reference list, and the APA 7th Edition guidelines. Subsequently, I made substantial revisions to all AI-generated content to ensure its accuracy, consistency with the research findings, and coherence with my own academic arguments. |

*You may use this free text box to explain the intent for the use of the AI generated content. For example, rather than stating what prompt(s) were used, you may articulate the purpose for which the prompt was used (supported by examples) here:*

I used AI as a support tool to improve the clarity, organisation, and presentation of my thesis. For example, I used AI to obtain guidance on appendix organisation, regression table presentation, APA 7th referencing consistency, academic wording, and consistency checks between empirical tables and written explanations. These uses were intended to support refinement and presentation only, not to replace my own research design, data collection, analysis, interpretation, or conclusions.

### STUDENT DECLARATION

*By signing you are confirming that the AI use stated in the table(s) above are accurate and follow AUT's recommended guidelines detailed in the AI Hub and Postgraduate Handbook.*

|                        |                                                                                                 |                 |
|------------------------|-------------------------------------------------------------------------------------------------|-----------------|
| Student Name: Ruiyu Li | Signature:  | Date: 27.7.2026 |
|------------------------|-------------------------------------------------------------------------------------------------|-----------------|

## **Chapter 1. Introduction**

### **1.1 Cybersecurity as a Corporate Reporting and Capital-Market Issue**

In the rapidly evolving digital economy, cybersecurity risk has evolved from a technical issue to a business and strategic concern, as high-profile incidents have made investors, regulators, and other market participants increasingly aware of the substantial financial, operational, regulatory, and reputational consequences of cyber failures (Amir et al., 2018; Kamiya et al., 2021; SEC, 2023). For example, Target disclosed a cybersecurity incident in its 2013 annual report in which attackers stole payment card data from approximately 40 million accounts (Target Corporation, 2014), and in 2017, Equifax initially announced in September 2017 that the breach potentially affected approximately 143 million U.S. consumers; subsequent analysis increased the affected population to approximately 147.9 million U.S. consumers (Equifax Inc., 2017, 2018). The WannaCry ransomware attack occurred across at least 150 countries (Reuters, 2017), and the SolarWinds breach subsequently prompted U.S. authorities to issue warnings that government agencies, critical infrastructure sectors, and private-sector organisations had all been affected (CISA, 2020). These incidents have elevated cybersecurity from a technical concern to a pivotal matter of corporate governance, external reporting, and capital-market assessment (Kiesow Cortez & Dekker, 2022; X. C. Chen et al., 2023; SEC, 2023). Cyber risk refers to the likelihood and potential impacts of cyber-related adverse events, whereas cybersecurity concerns the protection of information systems and digital assets from unauthorised access, disruption, modification, or destruction (NIST, 2024). As businesses become increasingly dependent on digital infrastructure, data-intensive operations, and interconnected business processes, firms are disclosing a broader range of cybersecurity-related information to external stakeholders (Adams & Moore, 2025; Gao et al., 2020; SEC, 2023). Such disclosures typically encompass material incidents, such as data breaches or ransomware incidents, cybersecurity risk management processes and board-level governance and oversight arrangements, and compliance with cybersecurity or data protection requirements (Gao et al., 2020; SEC, 2023). Annual reports and regulatory filings now routinely embed this information across risk-factor discussions, management commentary, and governance sections (Gao et al., 2020; SEC, 2023). This broadened scope of reporting matters because cybersecurity disclosure has moved far beyond breach announcements, serving as a primary channel

through which firms communicate their cyber-risk profile and risk-management capabilities to external stakeholders (Adams & Moore, 2025; J. Chen et al., 2023; Jiang et al., 2022).

Underpinning this disclosure trend, regulators and investors are increasingly recognising that a firm's cyber-risk exposure and the quality of its risk management are relevant not merely to immediate corporate value, but to operational continuity and long-term sustainability (SEC, 2011, 2023). For instance, the SEC has gradually developed its cybersecurity disclosure framework in the United States. It began with staff guidance in 2011, followed by interpretive guidance in 2018, and culminated in binding rules in 2023. These rules require annual disclosures on cybersecurity risk management, strategy, and governance in Form 10-K, together with current disclosure of material cybersecurity incidents in Form 8-K (SEC, 2011, 2018, 2023). Several major jurisdictions outside the United States exhibit a similar regulatory direction. For example, the European Union's General Data Protection Regulation (GDPR) introduced mandatory notification requirements for personal data breaches (European Parliament & Council of the European Union, 2016, Art. 33), and the Network and Information Systems Directive 2 (NIS2 Directive) extends cybersecurity risk-management and incident-reporting obligations to a broader range of essential and important entities, with explicit attention to supply-chain security. Australia's Prudential Standard CPS 234 Information Security, administered by the Australian Prudential Regulation Authority (APRA), imposes binding information security requirements on regulated institutions (APRA, 2019), and the Australian Securities Exchange (ASX) Corporate Governance Principles and Recommendations explicitly state that the boards of listed firms should oversee cyber risks as part of their governance responsibilities. China's Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021) collectively form a national framework for cybersecurity, data security, and personal information protection, with the Cyberspace Administration of China playing a central coordinating and enforcement role alongside other sectoral regulators. These developments indicate that heightened expectations regarding cyber-related reporting and incident notification are part of a broader international regulatory trend, rather than a phenomenon limited to a single market (Amani et al., 2025; Schmitz-Berndt, 2023).

Collectively, these regulatory developments establish increasingly formal expectations for corporate cybersecurity reporting and provide market participants with a broader information basis for assessing cyber risk.

Empirical finance research increasingly documents the capital-market consequences of these disclosures. Havakhor et al. (2026) find that disclosures of cybersecurity investments are associated with lower costs of accessing debt and equity capital, thereby lowering the overall cost of capital. This effect is stronger when disclosures are less boilerplate and more informative, and when they are supported by actual cybersecurity investments. Chai et al. (2011) further show that market responses to cybersecurity investment announcements vary with the nature and credibility of the information disclosed. These findings suggest that investors focus not only on whether cybersecurity information is disclosed, but also on the specificity, substance, and informativeness of the information provided. When firms communicate their cybersecurity risk exposure and risk-management capacity more transparently, investor uncertainty may be reduced and financing costs may decline (Healy & Palepu, 2001; Easley & O'Hara, 2004). Cybersecurity-related disclosure is not merely a reporting obligation, but also an increasingly important firm-level information variable with potential capital-market consequences (Gordon et al., 2010; J. Chen et al., 2023).

## **1.2 Informativeness of Cybersecurity Disclosures**

Building on these capital-market findings, recent research has examined whether cybersecurity risk disclosures provide information that helps investors assess a firm's cyber risk profile (J. Chen et al., 2023; Amani et al., 2025). Adams and Moore (2025) demonstrate an important practical limitation of disclosure informativeness. They find that disclosures are often buried in lengthy regulatory filings and expressed in general legal language, which limits their practical usefulness for investors, even when they meet formal disclosure requirements. This concern raises a central question: what distinguishes more informative disclosure from mere boilerplate?

This distinction is central to the capital-market evidence presented by Havakhor et al. (2026), who find that the cost of capital benefit associated with cybersecurity investment disclosure is concentrated in disclosures that provide more substantive information rather than those that simply add to disclosure volume. This finding indicates that investors do not simply reward greater disclosure quantity; they

respond to the quality and precision of the information provided. Generic boilerplate language may satisfy formal disclosure expectations while doing little to reduce investor uncertainty about a firm's actual cyber risk exposure or risk management capability (Healy & Palepu, 2001; Easley & O'Hara, 2004). This thesis defines the informativeness of cybersecurity-related disclosure as the extent to which disclosed content provides decision-useful information about the firm's actual cyber risk profile, governance arrangements, risk management measures, preparedness, and potential operational or economic consequences. This definition treats informativeness as a disclosure quality construct rather than a measure based solely on disclosure extent. Informative disclosure, consistent with disclosure-quality literature, decision-usefulness principles, and cybersecurity-specific regulatory guidance, should be sufficiently specific to avoid boilerplate reporting, materially relevant to the firm's actual profile and governance arrangements, and useful for external users' assessment of likely consequences (Beretta & Bozzolan, 2004, 2008; IASB, 2018; SEC, 2018, 2023).

This emphasis on specificity, relevance, and usefulness is grounded in the nature of cybersecurity risk and the limitations of disclosure quantity as a proxy for reporting quality (Beretta & Bozzolan, 2004; Beattie et al., 2004). Cybersecurity risk is technically complex, firm-specific, and often difficult for outside investors to assess without substantive information from the firm (SEC, 2023; Adams & Moore, 2025). Thus, informative cybersecurity disclosure should be specific enough to distinguish the firm's own cyber exposure, governance arrangements, controls, and response mechanisms from generic statements that could apply to almost any firm (Campbell et al., 2014; Hope et al., 2016). It should also be relevant in the sense that the disclosed content relates to economically meaningful issues, such as operational disruption, data loss, regulatory exposure, reputational damage, litigation risk, or business continuity (IASB, 2018; J. Chen et al., 2023; Adams & Moore, 2025). Finally, it should be useful to external users by helping them evaluate the firm's cyber-risk position, preparedness, and likely consequences (Miihkinen, 2013). These three attributes are therefore central to this thesis because they translate the broad idea of decision-useful disclosure into observable features of cybersecurity-related reporting.

For the purposes of this thesis, the three dimensions of informativeness are defined as follows:

(a) Specificity: the extent to which a disclosure identifies concrete cyber-related risk sources, governance responsibilities, incidents, controls, or consequence channels, rather than relying on vague or standardised language that could apply to almost any firm (Beretta & Bozzolan, 2004; Adams & Moore, 2025; Campbell et al., 2014; Hope et al., 2016),

(b) Relevance: the extent to which disclosed content addresses cyber issues that are economically meaningful for investor assessment, such as operational disruption, data loss, governance deficiencies, or exposure channels that could plausibly affect firm value, rather than disclosing cybersecurity information that is only tangentially connected to material business risk (IASB, 2018; Campbell et al., 2014; J. Chen et al., 2023), and

(c) Usefulness: the extent to which disclosed information enables outside users to form a more informed assessment of the firm's cyber-risk position and likely consequences, rather than merely signalling that management is aware of cybersecurity as a general topic (Healy & Palepu, 2001; Miihkinen, 2013; Verrecchia, 2001; IASB, 2018; Adams & Moore, 2025).

### **1.3 Cross-Country Drivers of Cybersecurity Disclosure Informativeness**

Although the previous section provided a conceptual explanation of informativeness in terms of specificity, relevance, and usefulness, these attributes are unlikely to be realised uniformly across jurisdictions (Bushman et al., 2004; Hope, 2003a; Leuz & Wysocki, 2016). This expectation is consistent with prior research in international accounting and disclosure, which suggests that the informativeness of corporate reporting is shaped by institutional context rather than by firm choice alone. Cross-country studies in the broader disclosure literature show that the quality and transparency of firm-level reporting vary systematically with country-level characteristics such as legal structure, enforcement strength, and the depth of the information environment (Bushman et al., 2004; Hope, 2003a, 2003b; Leuz & Wysocki, 2016). These findings indicate that disclosure is not equally informative across settings, even when firms discuss broadly similar topics.

While the cross-country evidence in the cybersecurity disclosure literature remains relatively limited, emerging studies point in a similar direction (Amani et al., 2025). Existing research similarly suggests that the amount and character of cybersecurity related disclosure are not determined solely by

reporting format or the presence of cyber risk itself (Amani et al., 2025; Barry et al., 2022). This pattern is illustrated by Barry et al. (2022), who find that Chinese firms cross-listed in the United States disclose less cybersecurity-related information than comparable U.S. domestic firms even under the same reporting regime. This indicates that cross-country comparison is meaningful in the cybersecurity setting and provides a basis for expecting that cybersecurity disclosure differences may reflect institutional factors rather than random variation.

Building on this observation, prior studies also suggest two broad reasons for such differences. One reason relates to the reporting environment firms face, including differences in regulatory expectations, enforcement strength, and the broader purpose of disclosure (La Porta et al., 2006; Hail & Leuz, 2006). International accounting research shows that disclosure quality varies across countries because regulatory systems differ in their emphasis on investor protection, transparency, and enforcement credibility (La Porta et al., 2006; Leuz et al., 2003; Hail & Leuz, 2006). In more investor-oriented environments, firms are more likely to face pressure to provide firm-specific, decision-useful information. In more compliance-oriented environments, disclosures may be more likely to satisfy formal requirements through standardised or cautious language without maximising substantive informational value. In the cybersecurity context, this means that disclosure may differ not only in quantity but also in the extent to which it is specific, relevant, and useful to investors.

A further consideration concerns how investors interpret and use the information provided. Informativeness depends not only on what firms disclose but also on whether market participants have the incentive and capacity to treat that information as relevant to firm risk assessment. Prior research suggests that the economic effect of disclosure depends on how investors process the information provided and whether they regard it as pricing-relevant (Diamond & Verrecchia, 1991; Hail & Leuz, 2006). Cybersecurity disclosures that are specific, relevant, and useful are more likely to influence capital-market outcomes in markets where firm-specific risk disclosure is more readily incorporated into investor assessments (Berkman et al., 2018; Havakhori et al., 2026). By contrast, where disclosure is more readily interpreted as formal compliance language, even substantively informative disclosure may be less fully incorporated into investor assessments and may therefore have weaker capital-market consequences. Australia and China provide contrasting institutional settings. Australia

operates within a common law market framework with a stronger investor protection orientation, whereas China combines capital-market disclosure requirements with a more prominent state and regulatory role in cybersecurity governance. This contrast provides a useful comparative setting for examining whether the informativeness and capital-market implications of cybersecurity disclosures differ between the two countries.

#### **1.4 Rationale for Comparing Australia and China**

The value of comparing Australia and China lies not only in their regulatory differences, but also in the fact that both markets have established corporate disclosure regimes and continue to develop their cybersecurity frameworks. However, the two markets may differ in how cybersecurity issues are reflected in corporate reporting and how the resulting disclosures are incorporated into investor assessments.

Australian-listed firms operate within an investor-oriented continuous disclosure regime. ASX Listing Rule 3.1 requires a listed entity to immediately disclose any information that a reasonable person would expect to have a material effect on the price or value of its securities, subject to the exceptions set out in Listing Rule 3.1A (ASX, 2024). The Australian Securities and Investments Commission (ASIC) describes the continuous disclosure obligations under the Corporations Act 2001 as fundamental to maintaining market integrity by ensuring transparency and equal access to information. Listed firms must also disclose material price-sensitive information on a timely basis and comply with the listing rules of the relevant market. ASIC may address breaches through enforcement mechanisms, including infringement notices (ASIC, n.d.). Furthermore, the ASX Corporate Governance Principles and Recommendations emphasise timely and balanced disclosure, board-level risk oversight, disclosure of governance arrangements, and periodic reviews of the effectiveness of risk-management frameworks. The commentary to Recommendation 7.2 explicitly identifies digital disruption, cybersecurity, privacy, and data breaches as contemporary and emerging risks that the board or a board committee should consider when reviewing the entity's risk-management framework (ASX Corporate Governance Council, 2019). Although Australia does not have an SEC-style standalone annual cybersecurity disclosure rule applying uniformly to all listed firms, ASIC's guidance indicates that directors may need to disclose cybersecurity risks and cyber incidents where they are

market-sensitive, material to the operating and financial review, or relevant to avoiding material misstatement in annual financial reporting (ASIC, 2022). Within this disclosure environment, material cybersecurity risks, governance oversight, and risk-management arrangements may be more readily incorporated into firm-level reports intended for investors.

On the other hand, there are significant differences in China's institutional approach to cybersecurity. The regulatory frameworks of China, which include the Cybersecurity Law, originally effective in 2017, the Data Security Law (2021), and the Personal Information Protection Law (2021), integrate cyber governance into a broader national-level framework centred on cyberspace sovereignty, national security, data security, and personal information protection. At the same time, Chinese listed firms are also required to operate under the formal securities information disclosure system. The Measures for the Administration of Information Disclosure by Listed Companies, issued by the China Securities Regulatory Commission (CSRC), aim to standardise information disclosure, strengthen disclosure management, and protect investors. The annual report content and format standards further require listed firms to disclose material risk factors based on firm-specific characteristics and to explain existing or planned mitigation measures. China does not lack investor-oriented information disclosure requirements. Beyond investor communication, however, the broader institutional environment places greater emphasis on regulatory compliance and state oversight. This distinction is crucial because broader cybersecurity regulation does not automatically imply that corporate-level annual report disclosures will be more informative. Although stricter regulation may increase formal reporting obligations, it may also encourage cybersecurity related matters to be incorporated into compliance oriented or standardised disclosure frameworks. Consequently, annual reports may place relatively less emphasis on firm-specific information intended to support investor decision making.

This distinction is relevant because the difference between Australia and China is not simply one of regulatory presence or absence, but of disclosure orientation, enforcement channels, and institutional emphasis. In Australia, material cyber-related issues may be more readily linked to continuous disclosure and governance communication directed toward investors, supported by a regime that emphasises timely market-sensitive disclosure, cyber risk oversight, and enforcement of disclosure obligations (ASX, 2024; ASIC, 2017, 2022). In China, by contrast, cyber governance is more visibly

embedded in a broader compliance and state supervision framework, even though listed firms remain subject to formal investor protection-oriented disclosure rules (CSRC, 2021a, 2021b; Standing Committee of the National People's Congress, 2016, 2021a, 2021b). Recent cross-country disclosure research also suggests that country level institutional factors help explain differences in the intensity, diversity, and informativeness of corporate disclosure, while risk disclosure research shows that enforcement strength materially affects disclosure compliance (Adam-Müller & Erkens, 2020; Liu et al., 2024). Viewed collectively, these considerations provide the institutional foundation for the empirical comparison that follows.

Beyond the institutional argument developed above, Barry et al. (2022) provide one of the most relevant cybersecurity-specific comparative reference points for the present study. Examining cybersecurity disclosures by Chinese firms cross-listed in the United States relative to U.S. domestic firms, they show that Chinese cross-listed firms disclose less cybersecurity-related information than their U.S. counterparts and interpret this pattern as consistent with cybersecurity being more strongly externalised through China's regulatory framework than communicated through firm-level disclosure. They also find that the market valuation effect of cybersecurity disclosure is context-dependent and sensitive to perceptions of institutional setting (Barry et al., 2022). Because this evidence is drawn from a U.S. cross-listing environment, it is most useful here not as a direct prediction of pricing effects in China's domestic market, but as cyber-specific evidence that institutional setting can shape both disclosure behaviour and the way markets respond to cybersecurity-related information. This interpretation is also consistent with broader non-financial and corporate disclosure evidence that country-level institutional and legal factors influence the informativeness of disclosure and the extent to which disclosure becomes reflected in market prices (da Silva, 2025; Liu et al., 2024). Thus, Barry et al. (2022) provide cyber-specific support for the view that institutional setting matters for cybersecurity disclosure, which reinforces the rationale for comparing Australia and China.

### **1.5 Research Gap and Motivation**

The existing cybersecurity disclosure literature has established that cybersecurity-related reporting matters to investors and capital-markets, but current knowledge remains incomplete in several important respects. Prior studies show that cyber-related disclosure may carry economic consequences

and that the institutional environment can shape disclosure practices and market responses. However, existing evidence remains concentrated in a limited set of settings, relies heavily on disclosure presence or volume-based measures, and provides only limited insight into whether annual-report cybersecurity-related disclosure is substantively informative and whether such informativeness matters similarly across countries.

First, the empirical evidence is heavily concentrated in the United States. Most studies rely on SEC filings, U.S. firm samples, or U.S.-based regulatory events, and the extent to which their findings generalise to other institutional settings remains largely untested (Amani et al., 2025; Barry et al., 2022). Non-U.S. evidence is limited, and cross-country evidence is rarer still. As a result, the field lacks sufficient understanding of how institutional context shapes disclosure practices and their capital-market consequences in settings outside the U.S. regulatory environment.

Second, the majority of existing studies focus on breach disclosure, short-window market reactions to cyber incidents, or the volume of cyber-related language in 10-K risk factor sections. While these approaches generate useful evidence about particular disclosure events or aggregate disclosure quantities, they do not directly address whether the substantive content of annual-report cybersecurity disclosure is informative. The disclosure informativeness question in a cross-country setting remains relatively underexplored (Adams & Moore, 2025; Amani et al., 2025).

Third, measurement in the cybersecurity disclosure literature has largely remained at the level of disclosure existence, word count, or keyword frequency. These approaches conflate disclosure volume with disclosure quality and are unable to capture whether disclosed content is specific, relevant, and useful to investors. As Beretta and Bozzolan (2004) argue in the broader risk disclosure literature, disclosure quality depends not only on how much is disclosed but on the substance of what is communicated. In the cybersecurity context, developing more substantive informativeness measures remains an important methodological challenge.

Fourth, the association between cybersecurity disclosure informativeness, understood as a multi-attribute construct, and the cost of equity has not been examined in an Australia-China comparative context. Havakhor et al. (2026) establish that more informative cybersecurity disclosures are associated with a lower cost of capital in the U.S., and Barry et al. (2022) demonstrate that the

institutional environment shapes disclosure patterns and market reactions. However, neither study examines cross-country variation in the relationship between informativeness and the cost of equity, using Australia and China as the comparative setting. This gap is significant given the contrasting institutional orientations of these two markets and because these institutional differences may influence how investors interpret and price cybersecurity disclosure.

Together, these four gaps motivate the present thesis. The study addresses them by focusing on the informativeness of cybersecurity-related disclosures in annual reports rather than their presence or volume, comparing Australia and China as institutionally distinct settings, examining the association between informativeness and the cost of equity, and testing whether that association differs between the two institutional settings.

## **1.6 Research Objectives and Research Questions**

This thesis pursues three interconnected research objectives. The first objective is to examine whether the informativeness of cybersecurity-related disclosure is higher in Australian-listed firms than in Chinese-listed firms, and to characterise any cross-country variation across the dimensions of specificity, relevance, and usefulness. The second objective is to test whether higher disclosure informativeness is associated with a lower cost of equity, as theory would predict. The third objective is to investigate whether the association between disclosure informativeness and the cost of equity differs between Australia and China, consistent with the institutional channels developed in Chapter 2.

The research questions are as follows:

*RQ1: Does the informativeness of cybersecurity-related disclosures differ between Australian-listed and Chinese-listed firms?*

*RQ2: Is higher cybersecurity-related disclosure informativeness associated with a lower cost of equity?*

*RQ3: Does the association between cybersecurity-related disclosure informativeness and cost of equity differ between Australia and China?*

These research questions are examined through three testable hypotheses developed in Chapter 2.

## 1.7 Methodology Preview

To examine both the informativeness of cybersecurity-related disclosure and the capital-market consequences, this thesis adopts a quantitative archival research design. The empirical setting consists of listed firms in Australia and Mainland China from FY2022 to FY2024. The final sample includes 100 Australian firms and 100 Chinese firms, producing 600 firm-year observations. Annual reports are used as the textual source for measuring cybersecurity-related disclosure because they provide a relatively standardised and comparable basis for measuring cybersecurity-related disclosure across the two institutional settings.

The first stage of the research design constructs the Cybersecurity-Related Disclosure Score (CSRDS). Cybersecurity-related passages are identified from annual reports using a Python-assisted bilingual keyword and anchor-based extraction procedure. The extracted passages are then evaluated using a codebook-based scoring framework that measures disclosure informativeness through three dimensions: Specificity, Relevance, and Usefulness. These dimensions are operationalised through nine indicators, each scored on a 0-2 ordinal scale. The final CSRDS measures are constructed at the firm-year level and include aggregate CSRDS, dimension-level scores, and indicator-level scores.

The second stage links CSRDS to capital-market outcomes. The dependent variable is the cost of equity, estimated with the CAPM with firm-level beta and country-year capital-market inputs. The empirical tests examine three issues: whether Australian firms provide more informative cybersecurity-related disclosures than Chinese firms; whether CSRDS informativeness is associated with the cost of equity; and whether this association differs between Australia and China. The main regression analyses use pooled OLS models with fiscal-year fixed effects, firm-level controls, and firm-clustered standard errors. Additional robustness and sensitivity analyses include broad industry fixed effects for the H1, H2, and H3 specifications, LSEG StarMine WACC as an alternative market-based financing-cost outcome, winsorised variables, a positive CSRDS indicator, positive-CSRDS subsample analyses, governance controls, and country-specific models. Multiple-testing adjustment is additionally applied to the indicator-level inference using Holm's method.

## 1.8 Research Contributions

This thesis extends cybersecurity disclosure research beyond the predominantly U.S.-centred setting by providing systematic cross-country evidence from Australia and China. Existing cybersecurity disclosure research remains strongly influenced by U.S. regulatory filings, cyber incident settings, and SEC-related disclosure requirements, yet comparative evidence across non-U.S. institutional environments remains limited (Amani et al., 2025; Barry et al., 2022). This thesis examines listed firms in Australia and China under their respective domestic reporting environments, treating the Australia-China comparison as a theoretically motivated institutional comparison rather than treating country merely as a background control variable. This design allows the study to examine not only whether firms disclose cybersecurity information, but also whether the informativeness and framing of such disclosure differ across national reporting environments. Additionally, this thesis develops and applies a codebook-based Cybersecurity-Related Disclosure Score (CSRDS) structured around three dimensions: Specificity, Relevance, and Usefulness. This framework provides a multidimensional operationalisation of cybersecurity-related disclosure informativeness by moving beyond disclosure presence, volume, or keyword frequency to examine specific disclosure attributes. A further contribution is the examination of the association between CSRDS informativeness and the cost of equity, which extends understanding of the capital-market relevance of cybersecurity disclosure quality. Prior research shows that cybersecurity-related disclosure can affect market valuation and that the content of disclosure matters in how investors interpret cybersecurity information (Barry et al., 2022; Berkman et al., 2018). This thesis builds on this literature to examine whether annual-report cybersecurity disclosure is associated with firms' equity financing costs across two non-U.S. institutional settings. Importantly, the study does not assume that aggregate cybersecurity disclosure is uniformly priced by the market. Instead, analysing CSRDS at the aggregate, dimension, and indicator levels distinguishes broad disclosure informativeness from specific attributes that may be more decision-useful to investors. This design clarifies whether the capital-market relevance of cybersecurity disclosure depends on general disclosure quality or on particular attributes, such as whether firms connect cyber risk to concrete business consequences, and thereby contributes to accounting disclosure research.

The remainder of the thesis proceeds as follows. Chapter 2 reviews the relevant literature and develops H1-H3. Chapter 3 describes the research design, sample selection, CSRDS construction, variable measurement, empirical models, and robustness tests. Chapter 4 reports the empirical results. Chapter 5 discusses the findings, contributions, and practical implications. Chapter 6 concludes the thesis, outlining its limitations and directions for future research.

## **Chapter 2. Literature Review and Hypothesis Development**

### **2.1 Conceptualising Cybersecurity-Related Disclosure Informativeness**

#### **2.1.1 Cybersecurity-related disclosure as a distinct and decision-relevant reporting domain**

There is an increasing number of accounting and finance studies that view cybersecurity-related disclosures as a distinct reporting area rather than merely a subset of general risk-related disclosures. Early research examined cybersecurity disclosure as part of broader technological or operational risk reporting, but recent systematic reviews indicate that the area has now developed sufficiently to warrant separate conceptual treatment (Amani et al., 2025; Haapamäki & Sihvonen, 2019). Several characteristics set cybersecurity risk apart from other categories of corporate risk. Cyber threats are technically complex and rapidly evolving, making it difficult for outside investors to independently assess a firm's exposure without detailed, firm-specific disclosure (Amani et al., 2025; SEC, 2023). Cybersecurity risk is also inherently cross-functional, spanning information technology, legal compliance, operations, governance, and strategy, as reflected in regulatory requirements that treat cybersecurity disclosure as a matter of risk management, strategy, governance, and incident reporting (SEC, 2023; Adams & Moore, 2025). The potential consequences of cyber incidents are diverse and often difficult to quantify in advance, encompassing operational disruption, data loss, reputational damage, regulatory penalties, and litigation exposure (Gao et al., 2020; J. Chen et al., 2023). Unlike many other risk categories, cybersecurity risk is shaped by adversarial behaviour: disclosure may interact with the risk it describes, since overly technical or security-sensitive disclosure could provide useful information to threat actors (SEC, 2023; Gordon et al., 2010). These features suggest that cybersecurity-related disclosure requires its own analytical framework rather than being subsumed under generic risk-factor analysis (Haapamäki & Sihvonen, 2019). Amani et al. (2025), in a comprehensive review of the cybersecurity disclosure literature, organise findings across disclosure characteristics, determinants, and outcomes, underscoring the need for conceptual clarity before the determinants and consequences of informativeness can be examined.

Systematic reviews of the broader risk-disclosure literature indicate that no single universally accepted definition of disclosure quality or informativeness yet exists, in part because prior studies adopt

different proxies and empirical approaches to operationalise the construct (Ibrahim et al., 2022; Mbithi et al., 2022). Prior literature generally treats disclosure informativeness as a functional construct whose meaning is inferred from whether disclosure improves users' understanding of firm risk, reduces uncertainty, and mitigates information asymmetry between managers and outside investors (Campbell et al., 2014; Ibrahim et al., 2022; Mbithi et al., 2022; Miihkinen, 2013). This functional interpretation is particularly useful in the cybersecurity context, where the key issue is not simply whether a firm mentions cybersecurity in an annual report, but whether the disclosed content enables external users to assess the firm's actual cyber risk profile.

This functional interpretation is consistent with two complementary perspectives on useful disclosure. The Conceptual Framework issued by the International Accounting Standards Board (IASB) states that financial information is useful when it is relevant to users' decisions and faithfully represents the economic phenomenon it purports to represent (IASB, 2018). Analytical and empirical disclosure research suggests a complementary view: corporate disclosure is informative when it reduces information asymmetry and helps capital-market participants assess firm-specific uncertainty, governance responses, and potential economic consequences (Healy & Palepu, 2001; Verrecchia, 2001; Leuz & Wysocki, 2016). In the cybersecurity context, merely mentioning cybersecurity risk is not sufficient: disclosure is useful only to the extent that it helps users assess the firm's exposure to future cyber-related adverse events and its response to such risks (H. Li et al., 2018; Adams & Moore, 2025). A disclosure may formally acknowledge cyber risk yet provide limited decision-usefulness if it does not explain the firm's specific exposure, governance arrangements, preparedness, or likely business consequences (Adams & Moore, 2025; H. Li et al., 2018).

The importance of distinguishing informativeness from mere disclosure presence is particularly acute in the cybersecurity setting, and recent evidence illustrates that the two are not synonymous (Adams & Moore, 2025; H. Li et al., 2018). Adams and Moore (2025) provide direct evidence on this point by examining the regulatory filings of 61 firms that experienced ransomware incidents between 2018 and 2021. They extract and classify 7,681 cybersecurity-related statements from 314 10-K filings and demonstrate that the substantive content of those disclosures varies substantially even within the same filing environment. Although firms commonly discuss prospective cyber risks, Adams and Moore

(2025) document more limited disclosure of risk mitigation strategies, incident response, and realised damages. For example, even after a ransomware incident, only 55% of affected firms discuss incident response in their filings, and ransomware is mentioned far less often in incident-response and proactive-mitigation statements than in prospective-risk or damage statements. This evidence shows that the presence of cybersecurity-related text in an annual report is not a reliable indicator of disclosure informativeness, highlighting the empirical gap between disclosure presence and decision-useful content that motivates the analysis that follows.

### **2.1.2 Prior Measures of Disclosure Informativeness and Their Limitations**

Existing studies have employed several different proxy measures to assess the informativeness of disclosures, with each measure reflecting a different aspect of the reporting environment. One common starting point is disclosure quantity, including word counts, disclosure length, sentence counts, page counts, and keyword frequency. The underlying intuition is that firms devoting more reporting space to a topic may be providing more information (Botosan, 1997; Hooks & van Staden, 2011; F. Li, 2008).

In the cybersecurity context, Gao et al. (2020) used keyword-based and content-analysis methods to identify and characterise cybersecurity-related disclosures in 10-K filings, and Calderon and Gao (2022) applied text-analysis techniques in a cross-country setting to compare the length, readability, numerical content, uncertainty, and litigious tone of cybersecurity risk disclosures made by U.S. and foreign firms. Studies employing these quantitative proxy variables indicate that the volume of cybersecurity disclosures is associated with firm size, industry membership, prior cybersecurity breaches, SEC guidance, and broader cybersecurity risk conditions (Gao et al., 2020; H. Li et al., 2018). Regarding disclosure outcomes, information security and cybersecurity disclosures have been associated with market value, bid ask spreads, firm performance, and measures of information asymmetry (Gordon et al., 2010; Al Amosh & Khatib, 2025). These findings indicate that disclosure quantity captures a meaningful dimension of the information environment, even if it does not fully distinguish substantive disclosure from boilerplate text.

Another strand of the literature shifts attention from disclosure quantity to the thematic content and tone of the disclosures. For example, Loughran and McDonald (2011) find that features specific to financial texts, including language expressing negativity and uncertainty, are associated with return volatility and trading volume. Their findings indicate that textual content conveys information that cannot be captured by simple word counts alone. In the cybersecurity setting, keyword-based and textual approaches similarly help identify the extent, emphasis, and content profile of cyber-related disclosures across firms and filing environments (Gao et al., 2020; Calderon & Gao, 2022). These approaches are useful for capturing thematic variation, but they remain limited in distinguishing firm-specific substantive content from standardised or templated disclosure language (Adams & Moore, 2025; Cheong et al., 2021; Gao et al., 2020).

Readability is another widely used metric. Readability studies examine how easily investors can process information disclosed in annual reports. F. Li (2008) shows that firms with poorer earnings performance produce less readable annual reports, consistent with managerial obfuscation, whereas Loughran and McDonald (2014) caution that general-purpose readability measures must be interpreted with care in financial reporting contexts. Ajina et al. (2016) and Lo et al. (2017) find that less readable reporting is associated with earnings management. Determinants and correlates of readability in this literature include firm performance, earnings management, and reporting complexity. Less readable or more complex reporting is generally associated with higher processing costs and weaker information accessibility for investors (F. Li, 2008; Loughran & McDonald, 2014; Miller, 2010; Lo et al., 2017). Some studies further link annual report disclosure characteristics to information asymmetry; however, direct evidence on readability itself remains mixed. This mixed evidence may stem from the fact that readability reflects an important aspect of report accessibility, yet readability alone does not determine whether the disclosed content is concrete, firm-specific, or substantively useful (Beretta & Bozzolan, 2004; Loughran & McDonald, 2014; Adams & Moore, 2025).

A more granular approach relies on researcher-coded content analysis, in which disclosure is evaluated against a predefined scoring framework. Beretta and Bozzolan (2004) provide an influential multidimensional approach to risk disclosure by distinguishing between the quantity and richness of content, while Miihkinen (2013) extends this logic by developing a disclosure index that captures

multiple facets of risk-reporting quality. In the cybersecurity domain, Adams and Moore (2025) similarly classify cyber-related statements at the content level, for example, by distinguishing among different types of cyber disclosures and assessing whether they contain firm-specific information rather than merely topical references. Research in this tradition suggests that content-level disclosure quality is shaped by governance characteristics, regulatory requirements, and institutional disclosure environments (Miihkinen, 2012; H. Li et al., 2018; Gao & Calderon, 2025; Zheng et al., 2025), and that higher-quality disclosure is associated with lower information asymmetry, more informative capital-market assessments of firm risk and value, and improved analyst forecast properties (Beretta & Bozzolan, 2008; Campbell et al., 2014; Miihkinen, 2013).

Other studies infer disclosure informativeness indirectly from analyst behaviour, market outcomes, or country level information environment measures. Analyst forecast accuracy, transparency indices, and related measures have been used as indirect indicators of disclosure quality in cross-country research (Hope, 2003a; Bushman et al., 2004; Leuz & Wysocki, 2016). More recent studies use textual analysis, factor analysis, machine learning, and natural language processing to classify cybersecurity disclosure content at scale (Cheong et al., 2021; Kesari, 2022; Amani et al., 2025). These approaches offer valuable evidence on the broader information environment and improve the scalability of textual classification. However, they do not necessarily identify whether disclosed cybersecurity content is specific, relevant, and useful to investors assessing a firm's actual cyber risk profile.

Each of the methods discussed above has made a valuable contribution to our understanding of the informativeness of disclosures, and together they have laid a solid empirical foundation for this field. The quantity-based measures have indicated that the extent of disclosure is associated with substantive outcomes in capital markets, including cost of equity, market value, liquidity, and information-asymmetry-related measures (Botosan, 1997; Gordon et al., 2010; Lang & Stice-Lawrence, 2015). Readability proxy variables suggest that the comprehensibility of disclosed information is important for investors' processing costs and information accessibility (Loughran & McDonald, 2014). Content analysis methods have enabled researchers to capture the actual content of disclosures rather than relying solely on quantity or readability proxies. Market and analyst-based proxy variables link disclosure characteristics to broader outcomes within the information

environment. However, quantity-based measures, while informative, may not fully distinguish between substantive and boilerplate content when firms engage in lengthy discussions of digital risk without providing firm-specific information about their own exposure, governance arrangements, or preparedness (Beretta & Bozzolan, 2004; Ibrahim et al., 2022; Mbithi et al., 2022; Adams & Moore, 2025). Readability-based proxies, while capturing an important dimension of accessibility, may not on their own indicate whether the disclosed content is concrete, firm-specific, or substantively useful, because a short and moderately technical cyber disclosure may be highly informative if it identifies concrete risk sources, governance responsibilities, or consequence channels (Adams & Moore, 2025; Beretta & Bozzolan, 2004). Keyword-counting and dictionary-based approaches, while effective at capturing thematic emphasis and cross-sectional variation, may struggle to distinguish between firm-specific substantive content and templated language derived from regulatory guidance or common industry practice (Adams & Moore, 2025; Gao et al., 2020; H. Li et al., 2018). Among the available approaches, content analysis offers the most direct basis for capturing the substance of disclosure, though its cross-country application requires a carefully specified coding framework to ensure comparability across institutional settings (Beretta & Bozzolan, 2004; Calderon & Gao, 2022). Given these complementary strengths and individual limitations, the present study adopts a multidimensional framework that focuses on the substance and investor orientation of disclosed content, rather than relying on any single surface-level proxy.

### **2.1.3 The framework of informativeness: specificity, relevance, and usefulness**

Building on the conceptual foundation established in Section 2.1.1 and the measurement limitations identified in Section 2.1.2, this study adopts a three-dimensional framework to operationalise the informativeness of cybersecurity-related disclosures. In this study, cybersecurity-related disclosure informativeness refers to the extent to which disclosed content provides information useful for assessing the firm's cyber-risk profile, including its exposure, governance arrangements, risk-management mechanisms, preparedness, and potential operational or economic consequences (Adams & Moore, 2025; Beretta & Bozzolan, 2004; H. Li et al., 2018; SEC, 2023). This definition treats informativeness as a disclosure-quality construct rather than a disclosure-volume construct

(Beretta & Bozzolan, 2004; Adams & Moore, 2025). The construct comprises three dimensions: specificity, relevance, and usefulness, each of which will be discussed separately.

The first attribute is specificity. Prior risk-disclosure research suggests that disclosure quality depends not only on the amount of disclosure but also on whether the disclosed information is concrete, firm-specific, and sufficiently detailed to distinguish one firm's risk profile from another (Beretta & Bozzolan, 2004; Campbell et al., 2014; Miihkinen, 2013). Specificity is particularly salient in the cybersecurity setting because generic references to "cyber attacks" or "information-security risk" provide limited insight into the nature of a firm's actual exposure (Adams & Moore, 2025; Gao et al., 2020; H. Li et al., 2018). A more specific disclosure identifies concrete threat types, risk-management mechanisms, or critical assets and systems (Adams & Moore, 2025; SEC, 2023). In this sense, specificity helps distinguish substantive cybersecurity disclosure from standardised or boilerplate risk language (Beretta & Bozzolan, 2004).

The second attribute is relevance. In the IASB Conceptual Framework, information is relevant when it is capable of making a difference to users' decisions (IASB, 2018). In the context of cybersecurity-related disclosure, relevance concerns whether the disclosed cyber issue is economically meaningful for investor assessment (IASB, 2018; SEC, 2023). This does not mean that all cyber-related text is relevant. A disclosure is more relevant when it addresses cyber matters that could plausibly affect operations, governance, regulatory exposure, business continuity, supply-chain resilience, reputation, litigation risk, or firm value (Adams & Moore, 2025; Gao et al., 2020; SEC, 2023). Thus, relevance captures the economically meaningful connection between the disclosed cyber issue and the firm's risk profile (IASB, 2018; SEC, 2023).

The third attribute is usefulness. Usefulness is related to relevance but conceptually distinct from it. Whereas relevance concerns whether the disclosed issue is economically meaningful, usefulness concerns whether the disclosure provides evaluative evidence that enables external users to assess the firm's exposure, preparedness, or realised outcomes (IASB, 2018; Beretta & Bozzolan, 2004; Miihkinen, 2013). A cyber disclosure may address a relevant topic, such as business interruption or cyber governance, but still provide limited usefulness if it offers no quantified resources, insurance

information, or details about incidents and their outcomes (Adams & Moore, 2025; H. Li et al., 2018; SEC, 2023). More useful disclosure provides evaluative detail, such as quantified cybersecurity resources, cyber insurance arrangements, or information about incident frequency, duration, losses, and other realised outcomes. Such information enables users to assess the firm's preparedness, exposure, and likely consequences more directly (Adams & Moore, 2025; H. Li et al., 2018; SEC, 2023).

Together, specificity, relevance, and usefulness capture three different aspects of disclosure informativeness. Specificity addresses whether the disclosure is firm-specific rather than generic; relevance addresses whether the disclosed issue is economically meaningful; and usefulness addresses whether the information enables external assessment. This three-dimensional framework is therefore well suited to the cybersecurity setting, where annual-report disclosures may range from brief boilerplate statements to detailed, firm-specific explanations of cyber exposure, governance, preparedness, and potential consequences. It provides the conceptual basis for examining whether CSRDS informativeness differs between Australia and China.

## **2.2 Literature for H1: Cross-Country Differences in CSRDS Informativeness**

### **2.2.1 Institutional Drivers of Disclosure Informativeness Across Countries**

The informativeness of cybersecurity-related disclosures may vary by country, as firms operate within different regulatory and institutional environments that determine what constitutes lawful, appropriate, and sufficient corporate communication. This logic is consistent with institutional theory. Institutional theory suggests that organisational practices are influenced by efficiency considerations as well as by the broader institutional context that defines appropriate behaviour (DiMaggio & Powell, 1983; Scott, 2008). Disclosure practices are shaped not merely by rational cost-benefit calculations at the firm level, but also by formal rules, enforcement structures, normative expectations, and cultural-cognitive patterns within the reporting environments of different countries. Relevant cross-national empirical studies confirm that corporate transparency exhibits systematic variations depending on the national-level information environment, including legal, judicial, and political structures (Bushman et al., 2004).

International research further indicates that national institutions are important determinants of corporate reporting quality and the broader information environment. This legal-institutional logic applies to disclosure because investor protection and enforcement shape managers' incentives to provide transparent information to outside users, as reflected in cross-country evidence on earnings management, corporate transparency, and analyst forecast accuracy (Bushman et al., 2004; Hope, 2003a; Leuz et al., 2003). Leuz et al. (2003) extend this logic to financial reporting quality, finding that firms in countries with stronger investor rights and more rigorous law enforcement engage in less earnings management, a pattern consistent with higher financial reporting quality. Hope (2003a) provides more direct evidence based on disclosure practices, showing that disclosure practices and the enforcement of accounting standards are associated with improved analyst forecast accuracy across countries. La Porta et al. (2008) note that the legal tradition systematically shapes a country's legal rules, regulations, and enforcement, providing a structural explanation for cross-national differences in disclosure outcomes. Collectively, these studies suggest that investor protection, enforcement strength, and legal origin are important institutional determinants of reporting and disclosure quality.

More recent cross-country evidence from Liu et al. (2024), based on firms from 35 countries, shows that country-level institutional factors help explain the intensity and diversity of corporate disclosures as well as their informativeness, meaning the extent to which disclosures convey substantive, decision-useful content. This evidence suggests that the institutional environment influences not only whether firms disclose information but also the substance of what they disclose, precisely the dimension of interest here.

Institutional theory also clarifies the mechanism through which country-level differences are translated into firm-level disclosure behaviour. Following DiMaggio and Powell (1983), firms are subject to three distinct forms of institutional pressure: coercive pressures arising from laws, regulators, and exchange rules that mandate or constrain certain disclosure practices; mimetic pressures arising from imitation of reporting practices that are regarded as legitimate or appropriate under conditions of uncertainty; and normative pressures arising from professional expectations embedded in accounting standards, auditing norms, and governance codes. Consistent with this mechanism-based perspective,

Depoers and Jérôme (2020) provide disclosure-based evidence that coercive, normative, and mimetic isomorphisms are each associated with variation in corporate disclosure levels.

Applied to cybersecurity-related disclosure, this institutional logic implies that country-level environments should shape not only whether firms disclose cyber-related information but also whether such disclosure is specific, relevant, and useful to investors, that is, whether it is informative in the three-dimensional sense developed in Section 2.1.3. In more investor-oriented disclosure environments, firms may face stronger coercive and normative pressures to provide timely, specific cyber-related discussion that anticipates investors' information needs. Where reporting is oriented more toward regulatory compliance than investor communication, firms may have stronger incentives to rely on cautious, standardised, or formally sufficient language that satisfies disclosure thresholds without maximising the specificity, relevance, or usefulness of the information conveyed. This institutional logic provides the theoretical basis for expecting cross-country differences in the informativeness of cybersecurity-related disclosure and anchors the empirical comparison between Australia and China developed in subsequent sections.

### **2.2.2 Empirical evidence on cybersecurity disclosure: single-country and cross-country studies**

To evaluate the empirical plausibility of this theoretical expectation, this section reviews single-country and cross-country evidence on cybersecurity disclosure informativeness.

#### **Single-country evidence**

Early cybersecurity disclosure research focused largely on single-country studies, particularly in the United States, where the literature initially mapped the content, determinants, and market relevance of cybersecurity-related disclosures within a single reporting environment. While this body of work established cybersecurity disclosure as an identifiable reporting domain, it offered limited direct insight into how disclosure informativeness might vary across institutional settings.

A foundational set of U.S. studies examined the impact of regulatory guidance on cybersecurity disclosure practices. H. Li et al. (2018) examine cybersecurity-related risk factors in 10-K filings around the SEC's 2011 staff guidance and show that regulatory guidance was associated with a

substantial increase in cybersecurity risk disclosure. They also find that the presence and length of cybersecurity risk disclosures were informative about future reported cybersecurity incidents in the pre-guidance period, but that disclosure presence became less informative after the guidance. This suggests that formal guidance may increase the incidence of disclosure without necessarily improving its informativeness. Adams and Moore (2025), in a detailed statement-level analysis of ransomware-affected firms, show that even within a common regulatory environment, disclosure varies substantially in specificity and substance. This finding reinforces the importance of measuring informativeness rather than treating disclosure as a binary variable. Collectively, these studies suggest that even within a single regulatory environment, cybersecurity disclosure varies in substantive content and cannot be treated as a uniform reporting practice.

More recent country-specific studies extend the evidence base to other jurisdictions. Al Amosh and Khatib (2025), focusing on Australia, find that greater cybersecurity disclosure among S&P/ASX 300 firms is positively associated with firm performance, a pattern consistent with lower information asymmetry. Andrew et al. (2026) show that ASX data breach disclosures are often limited in detail and that the materiality of such events may evolve as stakeholders react. These findings indicate that cybersecurity disclosure has information-environment consequences in Australia, though challenges remain in disclosure detail and materiality assessment. Zheng et al. (2025) document that audit committee IT expertise is positively associated with the quality of cybersecurity risk disclosure in China, suggesting that governance arrangements shape disclosure content within the Chinese institutional environment. These studies suggest that cybersecurity disclosure content is associated with governance and reporting conditions within individual countries and cannot be assumed to be uniform across settings.

### **Cross-country evidence**

While single-country studies provide indirect evidence that institutional conditions shape disclosure, cross-country studies offer more direct comparisons. An increasing number of studies have examined differences in cross-country cybersecurity disclosures by comparing firms operating in different regulatory environments. Lang and Stice-Lawrence (2015) provide broader evidence that textual

attributes of annual reports vary systematically across countries, including disclosure length, boilerplate language, comparability, and complexity. Calderon and Gao (2022) extend this comparative logic to cybersecurity-related disclosure, identifying systematic textual differences between U.S. 10-K filings and foreign 20-F filings, particularly in disclosure length and numerical content. They also find that foreign firms' cybersecurity disclosures tend to be clearer and more specific in certain respects than those of comparable U.S. domestic firms. These findings are relevant because more concrete, quantitatively supported, and specific disclosure is generally more likely to be decision-useful than vague or boilerplate language.

Barry et al. (2022) provide particularly important evidence for the present study by explicitly linking cross-country differences in cybersecurity disclosure to institutional factors. They show that Chinese firms cross-listed in the United States provide less cybersecurity-related disclosure than comparable U.S. domestic firms, and argue that this pattern reflects differences in the institutional setting rather than firm-level choices alone. Their findings also indicate that the market valuation of cybersecurity disclosures is higher for Chinese cross-listed firms, suggesting that the capital-market interpretation of cybersecurity disclosure depends on institutional context rather than disclosure quantity alone. This insight implies that the same quantity of disclosure may carry different meanings across institutional settings, and consequently, a cross-country comparison of informativeness requires attention not merely to how much is disclosed but to whether what is disclosed is specific, relevant, and useful in each setting.

Overall, the existing empirical evidence supports the view that cybersecurity disclosure quality is shaped by broader country-level reporting environments rather than solely by firm-level choice. At the same time, an important limitation of the extant literature is that most cross-country comparisons have been conducted within the SEC's common reporting environment, comparing U.S. domestic firms with foreign cross-listed firms. Evidence derived from a common SEC filing environment cannot be directly generalised to firms' home-country annual-report settings outside the SEC regime. Whether the informativeness of cybersecurity-related disclosure in annual reports differs systematically between firms operating in distinct home-country regimes, such as Australia and China, therefore remains an open question.

### 2.2.3 Australia and China as Contrasting Institutional Settings

The selection of Australia and China as the two focal countries is motivated by theoretically relevant institutional contrasts rather than geographic convenience. Prior literature and recent regulatory developments suggest that cybersecurity disclosure has become an increasingly formalised reporting domain, and recent international evidence shows that national-level institutions shape the intensity and diversity of corporate disclosure as well as its informativeness (Amani et al., 2025; Liu et al., 2024). Australia and China constitute a theoretically meaningful comparison, as prior literature and official regulatory frameworks point to differences in disclosure orientation, enforcement logic, and information environment.

At the regulatory level, the Australian disclosure environment is strongly market-facing and investor-oriented. ASX Listing Rule 3.1 requires listed entities to immediately disclose market-sensitive information, subject to limited exceptions, and ASX Guidance Note 8 explains the operation of this continuous-disclosure regime (ASX, 2024; ASIC, 2017). Empirical evidence supports this institutional logic. Shams et al. (2024) find that more extensive disclosure in M&A announcements is positively associated with market reactions, suggesting that investors perceive such disclosure as informative. X. C. Chen et al. (2023) show that sanctions for disclosure violations generate spillover effects on industry peers' liquidity. In the cybersecurity domain, Al Amosh and Khatib (2025) document a positive association between cybersecurity disclosure and firm performance (accounting- and market-based), which they interpret as consistent with lower information asymmetry. However, these studies primarily examine the quantity or aggregate effect of disclosure; they do not directly assess whether the disclosed content is specific, relevant, or decision-useful. Thus, while the Australian regime creates strong pressure for timely public communication, whether such pressure actually translates into disclosures that are substantively informative remains an open empirical question.

By contrast, studies of the Chinese reporting environment suggest a relatively stronger emphasis on regulatory supervision, standardisation, and compliance-based disclosure discipline. The survey evidence reported by Lu et al. (2023) indicates that Chinese firms view public voluntary disclosure as less relevant for reducing the cost of capital, partly because private communication channels with

connected stakeholders may reduce the capital-market role of public disclosure. This evidence indicates that, under different institutional environments, the disclosure function of annual public reports may not serve the same role in capital-market communication. Enforcement evidence points in a similar direction. Cao et al. (2021) find that informal securities enforcement is associated with fewer subsequent annual report restatements and that the two mainland stock exchanges have a stronger association with disclosure quality than central or local securities regulators. Using a randomised inspection policy, Jiang et al. (2025) find that inspections improve incremental disclosure quality by strengthening internal control oversight and deterring violations. This pattern is broadly consistent with China's official information-disclosure and cyber-governance frameworks: the relevant listed-firm disclosure rules emphasise the standardisation and management of disclosure, while the Cybersecurity Law and Data Security Law embed cyber governance within broader concerns of data security, national security, and public interest. Collectively, these studies suggest that the public disclosure environment of Chinese listed firms is more strongly shaped by regulatory oversight and compliance incentives than by a predominantly investor-facing disclosure logic, meaning that the pressures on firms to produce timely, specific, and investor-oriented communication are relatively weaker. However, similar to the Australian evidence, these Chinese studies primarily focus on enforcement effects or aggregate disclosure quality; they do not directly test whether the resulting disclosures meet the specificity, relevance, and usefulness criteria defined earlier.

The institutional contrast between Australia and China is further supported by broader comparative disclosure evidence. Brockman et al. (2023) examine Chinese firms listed in both mainland China and Hong Kong and find that the same firm discloses significantly more negative risk information in Hong Kong annual reports than in its mainland filings. This finding is particularly instructive because it holds firm identity relatively constant, making the observed divergence less likely to be driven solely by firm-level characteristics and more consistent with reporting-environment effects. Although this evidence concerns broader risk disclosure rather than cybersecurity disclosure specifically, it is consistent with cybersecurity-specific comparative studies showing that cyber-risk disclosure varies across institutional and filing environments (Barry et al., 2022; Calderon & Gao, 2022). Collectively, this evidence supports the view that institutional settings shape not only how much risk-related

information is disclosed, but also how that information is framed and how informative it is likely to be to outside users.

On this basis, Australia and China provide a theoretically meaningful setting for examining whether the informativeness of cybersecurity-related disclosure varies across domestic reporting environments and this study directly addresses that question by applying the three-dimensional framework of specificity, relevance, and usefulness to disclosures from both jurisdictions.

**Table 2.1***Institutional Comparison of Disclosure Orientation in China and Australia*

| Feature                                | China                                                                                                                                                     | Australia                                                                                                                                                     | Supporting sources                                                                                                                                                                                                                                |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulatory orientation                 | Rules-based and regulator-centred disclosure framework, with stronger emphasis on disclosure management, standardisation, and regulatory supervision.     | Principles-based and market-facing continuous disclosure framework, with stronger emphasis on timely release of price-sensitive information to the market.    | CSRC Regulations on Information Disclosure of Listed firms; CSRC Administrative Measures for Information Disclosure of Listed firms; ASX Guidance Note 8; ASIC guidance on handling corporate information.                                        |
| Relative institutional emphasis        | Data security, regulatory control, information management, investor protection, and broader public or national security interests.                        | Investor protection, market integrity, transparency, equal access to information, and pricing efficiency.                                                     | Cybersecurity Law of the People's Republic of China; Data Security Law of the People's Republic of China; Personal Information Protection Law of the People's Republic of China; CSRC disclosure regulations; ASX Guidance Note 8; ASIC guidance. |
| Relative public-disclosure orientation | Public disclosure is formally required, but cyber-related governance is also embedded in a broader regulatory and state-supervision framework.            | Public disclosure is primarily oriented toward the market as a whole through timely announcement of material price-sensitive information.                     | CSRC disclosure regulations; Cybersecurity Law; Data Security Law; ASX Listing Rule 3.1; ASX Guidance Note 8; ASIC guidance.                                                                                                                      |
| Typical public-disclosure logic        | Whether the matter meets prescribed securities disclosure requirements, regulatory reporting thresholds, or cyber/data governance obligations.            | Whether the information would reasonably be expected to have a material effect on the price or value of securities.                                           | CSRC disclosure regulations; Securities Law of the People's Republic of China; Cybersecurity Law; ASX Listing Rule 3.1; ASX Guidance Note 8.                                                                                                      |
| Likely emphasis in public reporting    | Compliance with mandated obligations, formal disclosure management, standardised reporting procedures, and regulatory administration.                     | Timeliness, firm-specificity, investor communication, and decision-usefulness for market participants.                                                        | CSRC disclosure regulations; Cao et al. (2021); Jiang et al. (2025); ASX Guidance Note 8; ASIC guidance; X. C. Chen et al. (2023); Shams et al. (2024).                                                                                           |
| Enforcement focus                      | Sanctions, regulatory measures, exchange-level monitoring, inspections, and compliance oversight for non-compliance with mandated disclosure obligations. | Enforcement of delayed, omitted, or misleading disclosure, with continuous disclosure treated as central to market integrity and equal access to information. | CSRC disclosure regulations; Cao et al. (2021); Jiang et al. (2025); ASIC guidance; ASX Guidance Note 8; X. C. Chen et al. (2023).                                                                                                                |

| Feature                                     | China                                                                                                                                                                                                                                                                                                                                                                     | Australia                                                                                                                                                                                                                                                                                                                                                                                                                     | Supporting sources                                                                                                                                                                                                                    |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cybersecurity-specific content requirements | Cybersecurity Law requires network operators to fulfil cyber-security protection and incident-reporting obligations; Data Security Law establishes data-security governance and classification obligations; Personal Information Protection Law governs personal-information handling; listed firms disclose material risks and events under securities disclosure rules. | No standalone cybersecurity-disclosure legislation applies uniformly to all listed firms. Instead, material cyber incidents or cyber-related risks may fall within ASX continuous disclosure obligations where price-sensitive; APRA CPS 234 imposes information-security requirements on APRA-regulated entities; corporate governance guidance encourages board oversight of material business risks, including cyber risk. | Cybersecurity Law of the People's Republic of China; Data Security Law; Personal Information Protection Law; CSRC disclosure regulations; ASX Guidance Note 8; APRA CPS 234; ASX Corporate Governance Principles and Recommendations. |
| Implication for CSRDS informativeness       | Cybersecurity-related annual-report disclosure may be more shaped by compliance, regulatory reporting, and standardised risk-management language, which can limit firm-specific, investor-oriented informativeness.                                                                                                                                                       | Cybersecurity-related disclosure is more likely to be linked to investor-oriented materiality assessment, governance communication, and timely market disclosure, which may encourage more specific, relevant, and useful disclosure.                                                                                                                                                                                         | Liu et al. (2024); Amani et al. (2025); Barry et al. (2022); Brockman et al. (2023); Al Amosh and Khatib (2025).                                                                                                                      |

*Source.* Author's compilation based on the official and academic sources cited in the final column.

*Note.* This table presents a stylised comparison of relative institutional emphasis relevant to cybersecurity-related annual-report disclosure. It does not provide an exhaustive description of all disclosure obligations in either country. The comparison should not be read as implying that China lacks investor-oriented disclosure rules or that Australia has a standalone cybersecurity disclosure regime for all listed firms. Rather, it summarises the regulatory and institutional features most relevant to the expected specificity, relevance, and usefulness of cybersecurity-related disclosures.

Overall, Table 2.1 summarises the institutional contrast that motivates H1. Australia's continuous-disclosure regime is more directly oriented toward timely market communication, while China's cyber-governance framework is more visibly embedded in regulatory supervision, data-security administration, and compliance management. These differences do not imply that China lacks investor-oriented disclosure rules, nor that Australia has a uniform standalone cybersecurity-disclosure regime. Rather, they suggest that Australian annual-report cybersecurity disclosures are more likely to be specific, relevant, and useful to external investors, whereas Chinese disclosures may be more strongly shaped by compliance-oriented and standardised reporting incentives.

#### **2.2.4 Research gap and H1 development**

There is a clear research gap that emerges from the literature review. Existing research on cybersecurity disclosure has primarily focused on single-country contexts or on cross-national comparisons within the common SEC reporting framework, particularly between Chinese and U.S. firms (Amani et al., 2025; Barry et al., 2022; Calderon & Gao, 2022). Although these studies indicate that institutional environments influence cybersecurity disclosure practices, they have not directly examined whether cybersecurity-related disclosures differ in informativeness between Australian and Chinese listed firms that file annual reports under their respective domestic regulatory regimes.

This research gap is significant for two main reasons. First, as discussed in Sections 2.2.1 and 2.2.3, the informativeness of disclosures is not equivalent to their volume, and it may vary independently across institutional environments. Second, evidence obtained under a common host-country reporting environment cannot be directly generalised to the context of annual report disclosures in the firms' home countries. Therefore, a direct comparison between Australia and China helps examine whether differences in domestic disclosure environments correspond to differences in the specificity, relevance, and usefulness of cybersecurity-related disclosures.

Based on the literature reviewed in Sections 2.1.2 through 2.1.3, existing research indicates that Australia and China provide different institutional incentives for public disclosure, and that such differences may influence the informativeness of cybersecurity-related disclosure (Liu et al., 2024;

Barry et al., 2022; Amani et al., 2025). Drawing on this literature, this study anticipates that cybersecurity-related disclosures by Australian listed firms will be more informative than those by Chinese listed firms. Therefore, the following hypothesis is proposed:

*H1: Cybersecurity related disclosure informativeness is higher for Australian listed firms than for Chinese listed firms, as reflected in greater specificity, relevance, and usefulness.*

## **2.3 Literature Review and Hypothesis Development for H2**

H2 examines the economic consequence of the informativeness of cybersecurity-related disclosure, more specifically, the cost of equity. This question is important because the informativeness differences identified in H1 matter only if they affect investors' required returns rather than simply changing how disclosure is presented. This section develops H2 by linking cybersecurity disclosure informativeness to information risk, capital-market pricing, and the broader empirical literature on disclosure quality and equity financing costs (Easley & O'Hara, 2004; Lambert et al., 2007; Botosan & Plumlee, 2002).

### **2.3.1 Literature and Research Gap**

#### **2.3.1.1 Cybersecurity Incidents and Market Outcomes**

Cybersecurity risk differs from many traditional sources of risk because a firm's cyber-risk exposure is largely hidden from outside investors, depending on internal systems, governance, and incident history that are not directly observable (Amir et al., 2018; Florackis et al., 2023). In the absence of reliable disclosure or realised incidents, investors cannot directly assess a firm's cybersecurity posture. Much of the existing literature has relied on market evidence to infer whether and how cyber risk is priced. Event-based studies document negative cumulative abnormal returns around cyber-breach announcements, suggesting that markets treat cybersecurity incidents as value-relevant events (Cavusoglu et al., 2004; Gatzlaff & McCullough, 2010; Gordon et al., 2011; Kamiya et al., 2021). Subsequent studies also suggest that the effects of cyber incidents can extend beyond short announcement windows. For example, studies report longer-run underperformance, elevated risk, increasingly negative cumulative abnormal returns, and longer-term changes in firm policies following

breaches (Ali et al., 2021; Chang et al., 2020; Hogan et al., 2023; Tosun, 2021). Other studies show that cyber incidents can deteriorate the information environment and reduce market liquidity, for example through wider bid-ask spreads and greater information asymmetry (Rosati et al., 2017). These findings imply that cybersecurity risk is relevant to investors and that markets respond when latent cyber risk is revealed through actual incidents.

However, this strand of research does not directly address the relevance of ex ante cybersecurity disclosure. Event-based studies examine the market's reaction after cyber risks materialise through actual incidents, but they do not address whether routine disclosure helps investors assess cyber exposure before such events occur. To examine that question, the next section reviews the literature on cybersecurity disclosure and its capital-market implications.

#### **2.3.1.2 Cybersecurity Disclosure and Market Outcomes**

Recent research has increasingly examined whether and how cybersecurity-related disclosures are associated with market and firm outcomes, extending attention beyond realised cyber incidents. Amani et al. (2025) classify prior cybersecurity disclosure studies according to disclosure characteristics, determinants, and outcomes, and identify market and firm outcomes as a major stream of this literature. The most relevant strands for H2 are those on stock market reactions, firm value, and other stock and debt market outcomes, especially studies that address financing costs or information asymmetry. Experimental investor studies also provide useful complementary evidence by showing whether particular disclosure attributes influence investment judgements. This section focuses on these most relevant strands before identifying the remaining research gap.

The first strand of research examines stock market reactions to cybersecurity-related disclosure, focusing mainly on short-window market responses. The evidence in this area is mixed, yet a clearer pattern emerges when studies are grouped according to the aspect of disclosure they measure. Studies using existence-based, quantity-based, or broad textual proxies—such as the presence, provision, length, or general tone of cyber-risk disclosure—tend to produce mixed evidence. Hilary et al. (2016) find limited changes in cyber-risk disclosure after breaches, while Morse et al. (2017) find that new cybersecurity risk-factor disclosures following SEC guidance are associated with negative stock price effects. J. Chen et al. (2023) show that increases in cybersecurity risk-factor disclosure after breaches

do not generate significant short-window market reactions, although decreases in such disclosure are associated with negative abnormal returns. Tsang et al. (2023) further show that sentiment types in risk-factor and MD&A disclosures can be informative, suggesting that even within broad textual measures, some attributes may matter. The balance of evidence in this first group indicates that investors do not respond systematically simply because cyber-related disclosure exists, is longer, or contains broad textual features such as aggregate tone or readability.

By contrast, studies that move beyond existence or volume and instead focus on the informational content of disclosure, that is, what it reveals about a firm's cyber conditions, actions, and exposures, tend to find more identifiable market effects. Gordon et al. (2010) find that voluntary information-security disclosures, particularly those concerning proactive security measures and specific vulnerabilities, are positively associated with firm market value. Chai et al. (2011) show that market reactions to information-security investment disclosures are more positive when the disclosures convey commercially relevant information. Florackis et al. (2023) further demonstrate that annual-report-based textual measures of cyber risk are associated with future stock returns. This evidence suggests that cybersecurity-related text can contain value-relevant risk information that is reflected in capital-market pricing over time, rather than only through immediate short-window reactions.

A further complication is that cybersecurity disclosure may not uniformly reduce investor uncertainty. Related evidence from broader capital-market outcomes shows that cyber-risk information can also reveal greater underlying exposure. For example, Jamilov et al. (2023) find that text-based cyber-risk measures drawn from conference calls are associated with higher implied volatility and variance risk premiums. This suggests that, in some channels or contexts, cybersecurity disclosure may amplify perceived risk rather than resolve uncertainty. Overall, this strand of evidence suggests that cybersecurity disclosure does not generate a uniform short-term market response. Rather, market reactions depend on what the disclosure reveals, how specific and commercially relevant it is, and whether investors interpret it as reducing uncertainty or as signalling greater cyber vulnerability. The critical distinction is therefore not how much is disclosed, but whether the disclosure is sufficiently informative to change investors' assessments of firm-level cyber exposure.

The second strand of research examines firm-value and valuation-related outcomes. Unlike short-window market reaction studies, this strand focuses on broader valuation measures, such as share price, market capitalisation, and Tobin's Q. The evidence is generally more favourable for disclosures that signal cybersecurity awareness, preparedness, or specific countermeasures, but it is not uniformly positive across disclosure channels and cyber-risk measures. Berkman et al. (2018) find that cybersecurity awareness, measured through the length and relevance of cyber-related disclosure in 10-K filings, is positively associated with both share price and Tobin's Q. Barry et al. (2022) similarly report that greater length and relevance of cyber disclosure are associated with higher share prices. Bose and Leung (2019) show that press-release disclosures of identity theft countermeasures have a positive long-term market value effect, while Gatzert and Schubert (2022) find that cyber risk management disclosures in annual reports are positively related to firm market value among financial institutions. However, valuation evidence based on cyber-risk exposure may point in a different direction. For example, Jamilov et al. (2023) show that conference-call-based cyber risk exposure is associated with stock returns, profits, and higher option market protection costs. Collectively, these studies suggest that investors may assign higher valuations when disclosure conveys preparedness, mitigation, or commercially meaningful information, but may discount firms when disclosure reveals greater underlying cyber exposure.

The third strand of research examines cost of capital and related stock and debt market outcomes. The evidence base is more limited but particularly relevant to the present study because it speaks more directly to whether cybersecurity disclosure is associated with investors' required returns. Havakhor et al. (2026) provide direct evidence that disclosure of cybersecurity investments in SEC filings is associated with lower cost of equity and debt. However, their primary disclosure variable captures whether firms disclose cybersecurity investments, and their additional informativeness tests focus on the non-boilerplate nature of those investment disclosures rather than a broader multidimensional measure of cybersecurity disclosure informativeness. Harris et al. (2023) find that the length, litigiousness, and lower readability of cyber-risk disclosure are associated with a higher cost of debt, suggesting that disclosure characteristics can also increase capital providers' risk assessments when they signal greater uncertainty or processing difficulty. Other studies examine adjacent outcomes related to information asymmetry and market uncertainty. Gordon et al. (2010) find that information

security disclosure is associated with narrower bid-ask spreads, and Berkman et al. (2021) show that more extensive cyber disclosure is associated with less informed trading ahead of earnings announcements. Jamilov et al. (2023) further show that text-based cyber-risk measures are associated with higher implied volatility and variance risk premiums. Collectively, these studies suggest that cybersecurity disclosure is associated not only with firm valuation but also the broader information environment on which capital-market pricing depends.

Experimental research on cybersecurity disclosure provides complementary evidence on how investors interpret disclosure characteristics. Bansal and Axelton (2024) find that more specific and verifiable disclosures increase nonprofessional investors' willingness to invest following a data breach. Huang and Murthy (2024) show that different types of cybersecurity risk-management strategy disclosures lead to different investor judgements and willingness to invest, while Gauch and Quick (2025) find that assurance statements and cyber insurance disclosures improve nonprofessional investors' investment responses. These studies suggest that investors attend not only to whether disclosure is present, but also to whether it appears credible, specific, verifiable, and decision-useful. Fortin and Héroux (2023) reinforce this interpretation by showing that experienced capital-market participants tend to view cyber-risk disclosure as boilerplate, unreliable, and lacking comparability across firms. Accordingly, the experimental and interview-based evidence suggests that disclosure characteristics matter, and that disclosure presence or quantity alone may not fully capture how investors interpret cybersecurity-related information.

Overall, two broad conclusions emerge from the existing literature. First, cybersecurity disclosure is associated with a range of market outcomes, including stock returns, firm value, information-asymmetry proxies, and financing-related measures. Second, the market consequences of disclosure appear to depend not only on whether disclosure is provided, but also on what the disclosure communicates. Boilerplate, highly standardised, or difficult-to-process disclosures tend to produce weaker or inconsistent effects, whereas more specific, relevant, credible, and decision-useful disclosures are more likely to influence investor judgements and market pricing (Bansal & Axelton, 2024; Fortin & Héroux, 2023; Gauch & Quick, 2025; Gordon et al., 2010; Harris et al., 2023; Huang & Murthy, 2024). This distinction is consistent with this study's CSRDS framework, which treats cybersecurity disclosure informativeness as a multidimensional construct rather than a simple

disclosure-presence or disclosure-length proxy. In particular, disclosure that links cybersecurity risk to operational or financial consequences may be especially relevant to investors because it translates technical cyber risk into assessable firm-level exposure. Existing studies, however, typically rely on relatively narrow proxies, such as disclosure presence, disclosure length, binary indicators of cybersecurity investment disclosure, or textual features such as readability and sentiment (Amani et al., 2025; Berkman et al., 2018; J. Chen et al., 2023). There is limited direct evidence on whether a multidimensional measure of annual report cybersecurity disclosure informativeness, capturing specificity, relevance, and usefulness, is associated with the cost of equity. The Australia-China setting remains especially underexplored in this respect.

### **2.3.2 Hypothesis Development**

#### **2.3.2.1 General Disclosure Quality and the Cost of Equity**

Because direct evidence on cybersecurity disclosure informativeness remains limited, the broader disclosure literature provides an important basis for assessing whether more informative disclosure is associated with lower required returns.

Botosan (1997) shows that greater annual-report disclosure is associated with a lower expected cost of equity, particularly among firms with relatively low analyst following. Lambert et al. (2007) further provide a theoretical basis for this relationship by showing that accounting information quality can influence the cost of capital both directly and indirectly. More recent research shows that disclosure effects depend not only on disclosure quantity but also on qualitative attributes. In the more specific context of risk disclosure, Beretta and Bozzolan (2004) argue that disclosure quality depends not only on the amount of information reported but also on its specificity and its ability to provide firm-level insights into risk exposure. Miihkinen (2013) finds that risk disclosures are more informative when they are detailed and closely linked to firms' actual risk conditions. Hope et al. (2016) further show that more specific qualitative risk-factor disclosures are associated with stronger market reactions and help analysts assess firms' underlying risk more effectively. Therefore, these studies suggest that higher-quality risk disclosure is not simply more extensive, but more specific, more closely connected to firm-level risk exposure, and therefore more useful to investors and analysts in assessing underlying risk.

### **2.3.2.2 Theoretical Mechanisms Linking Informativeness to the Cost of Equity**

This broader disclosure logic applies to cybersecurity-related disclosure because investors use cybersecurity disclosure to update their assessments of firm risk rather than pricing the disclosure itself. The relevant issue is whether disclosure explains the firm's specific cyber exposure, connects that exposure to economically meaningful consequences, and provides evidence that investors can use in assessing risk. However, cybersecurity disclosure differs from many general disclosure settings. Cyber risk is technical, largely hidden from outside investors, and shaped by internal systems and controls that are difficult to observe externally. More informative cyber disclosure may reduce uncertainty, but it may also reveal greater underlying exposure or raise adversarial concerns if detailed information can be exploited by malicious actors (Amir et al., 2018; Florackis et al., 2023; Jamilov et al., 2023). Whether the broader disclosure-quality argument extends to cybersecurity-related disclosure remains an empirical question.

Prior disclosure research generally suggests that more informative disclosure may reduce the cost of equity by lowering information risk. This line of argument is commonly grounded in information asymmetry theory, which holds that when managers possess private information unavailable to outside investors, investors face greater uncertainty about firm value and risk and therefore require a higher return to hold equity (Botosan, 1997; Lambert et al., 2007). This issue is particularly salient because outsiders cannot directly observe a firm's true cyber-risk exposure, the effectiveness of its internal cyber controls, the strength of its incident-response systems, or the quality of its board and managerial oversight. Accordingly, cybersecurity-related disclosure has been viewed as an important channel through which investors infer aspects of firms' cyber-risk management and exposure that are otherwise unobservable (Amir et al., 2018; Florackis et al., 2023; SEC, 2023). Kim and Pae (2025) further show that when information quality is uncertain, voluntary disclosure can communicate both expected cash flow implications and the precision of the underlying signal. In the present context, this reasoning suggests that investors may respond not only to whether cybersecurity information is disclosed but also to whether the disclosure appears sufficiently informative and precise. Informative cybersecurity disclosure may reduce information risk through three related channels: adverse selection mitigation, estimation risk reduction, and liquidity improvement. Specificity, relevance, and

usefulness may contribute to each channel and should not be treated as mechanically corresponding to separate mechanisms.

**(a ) Adverse selection mitigation**

Prior disclosure research suggests that more informative disclosure can mitigate adverse selection by narrowing the information gap between insiders and outside investors. This mechanism is consistent with Akerlof's (1970) "lemons" logic, under which outside investors discount assets when they cannot distinguish between higher- and lower-quality firms. In the disclosure literature, Healy and Palepu (2001) and Verrecchia (2001) similarly explain that disclosure can reduce this informational disadvantage by making firm conditions more visible to outside investors. Berkman et al. (2021) find that firms with lower cybersecurity risk mitigation scores experience greater pre-announcement informed trading, while Gordon et al. (2010) show that voluntary information-security disclosure is associated with narrower bid-ask spreads. Both findings are consistent with lower information asymmetry between more- and less-informed market participants and reduced adverse selection. This mechanism is not tied to relevance alone. Specificity helps investors distinguish firm-level cyber conditions from generic boilerplate language; relevance links cybersecurity information to the firm's actual cyber-risk exposure, governance arrangements, and risk-management capabilities. Usefulness provides evaluative evidence, including quantified cybersecurity resources, insurance arrangements, and information about incidents and realised outcomes. When these attributes are present, external investors are better able to distinguish firms with different cyber risk profiles and are less dependent on private information or unsupported assumptions. The return premium associated with informational disadvantage may therefore be lower.

**(b) Estimation risk reduction**

Informative disclosure can also reduce estimation risk by helping investors assess the likelihood and consequences of future cyber-related cash-flow disruptions (Barry & Brown, 1985; Lambert et al., 2007). This channel is particularly relevant when investors must evaluate not only whether cyber threats exist, but also how well the firm is positioned to detect, manage, and recover from them. Specificity may be especially important in this channel because it helps investors distinguish firm-specific cyber conditions from generic risk language. However, relevance and usefulness also contribute to estimation-risk reduction. Relevance helps investors connect cybersecurity issues to

firm-specific business consequences, such as operational disruption, customer relationships, regulatory exposure, and future performance. Usefulness further helps investors assess the potential magnitude or implications of those risks by providing information that can be incorporated into valuation judgements. The broader disclosure literature shows that more specific risk-factor disclosures are associated with stronger market reactions and improved assessments of firms' underlying risk (Hope et al., 2016). The cyber literature reviewed earlier is also consistent with the view that more substantive and firm-linked cyber disclosure is valued more highly by the market (e.g., Berkman et al., 2018; Gordon et al., 2010). Lambert et al. (2007) provide the theoretical foundation for this mechanism by showing that better-quality information can reduce the cost of equity by improving investors' assessment of the distribution of future cash flows. Disclosure that links technical cyber risk to operational or financial consequences may therefore be especially important because it translates a complex technical issue into assessable firm-level economic exposure.

### **(c) Liquidity improvement**

Informative disclosure is also more likely to improve liquidity when investors can use the information provided in valuation and trading decisions. Disclosure does not affect financing outcomes simply because it exists; it matters when investors can use it to interpret firm-level cyber exposure, assess the implications for future performance or risk management, and incorporate those judgements into valuation and trading decisions. This logic is consistent with Diamond and Verrecchia (1991), who argue that greater disclosure can reduce information asymmetry and improve market liquidity, and with Easley and O'Hara (2004), who show that assets with greater private information risk command higher expected returns. Usefulness is important because disclosure must be decision-relevant for investors to act on it. However, specificity and relevance are also necessary. Specificity makes disclosure less boilerplate and more comparable across firms, while relevance helps investors identify which cyber issues are economically material to the firm. Therefore, liquidity and market-processing benefits are more likely when cybersecurity disclosure is specific enough to reduce ambiguity, relevant enough to indicate firm-level exposure, and useful enough to support valuation and trading decisions. However, even potentially useful disclosure may fail to deliver these benefits if it is overly vague, excessively technical, or difficult to interpret, because investors then face higher information-processing costs. Readability affects investors' ability to process annual-report disclosure,

but it captures disclosure accessibility rather than the substantive informativeness of the disclosed content. Rjiba et al. (2021) show that annual-report readability is associated with the cost of equity. Readability is best treated as a facilitating condition for market processing rather than part of cybersecurity disclosure informativeness itself.

These mechanisms suggest that cybersecurity-related disclosure should not be treated as a single undifferentiated construct or as a simple disclosure-presence proxy. The three attributes of informativeness are complementary rather than mechanically tied to separate channels. Specificity reduces boilerplate ambiguity and helps investors identify firm-level cyber conditions; relevance connects cyber issues to actual risk exposure and business consequences; and usefulness helps investors evaluate the implications of disclosure for firm risk and valuation. These mechanisms help explain why more informative cybersecurity-related disclosure may reduce information risk and, in turn, be associated with a lower cost of equity.

**Table 2.2**

*Mechanisms Linking Disclosure Informativeness to the Cost of Equity*

| <b>Mechanism</b>               | <b>Description</b>                                                                        | <b>Key References</b>                                      |
|--------------------------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------|
| 1. Adverse Selection Reduction | Narrowing the information gap reduces the ‘lemons discount’ demanded by outside investors | Akerlof (1970); Healy and Palepu (2001); Verrecchia (2001) |
| 2. Estimation Risk Reduction   | More precise information improves assessment of future cash flows and systematic risk     | Lambert et al. (2007)                                      |
| 3. Liquidity Improvement       | Reduced information asymmetry lowers bid-ask spreads and transaction costs                | Diamond and Verrecchia (1991); Easley and O’Hara (2004)    |

### 2.3.3 Summary and Hypothesis Development for H2

The preceding sections establish three broad conclusions. First, cybersecurity risk is value-relevant: markets react negatively when hidden cyber risk is revealed through breach announcements (Cavusoglu et al., 2004; Gatzlaff & McCullough, 2010). Second, cybersecurity disclosure itself has capital-market consequences: more specific and informative disclosures are associated with higher firm valuations (Berkman et al., 2018; Gordon et al., 2010), narrower bid-ask spreads (Gordon et al.,

2010), lower cybersecurity risk mitigation is associated with greater informed trading before earnings announcements (Berkman et al., 2021), and lower cost of capital (Havakhor et al., 2026). Third, the broader disclosure literature supports the expectation that disclosure quality, rather than disclosure volume, is associated with lower required returns, and theoretical mechanisms explain how relevance, specificity, and usefulness may each contribute to this effect.

Despite these advances, direct evidence on whether cybersecurity disclosure informativeness affects the cost of equity remains limited and fragmented. Existing studies typically rely on relatively narrow proxies, including disclosure existence (Hilary et al., 2016), disclosure amount or changes in cyber-risk disclosure (J. Chen et al., 2023), textual cyber-risk exposure measures (Florackis et al., 2023), binary indicators of cybersecurity investment disclosure (Havakhor et al., 2026), or textual features such as readability and sentiment (Harris et al., 2023; Tsang et al., 2023). Only limited evidence examines a multidimensional annual-report informativeness construct that captures the specificity, relevance, and usefulness of cybersecurity-related disclosure as a composite measure. Furthermore, to the best of current knowledge, no study has tested such a relationship in a comparative setting involving Australian and Chinese listed firms, where differences in regulatory environments, investor composition, and information environments may shape how disclosure informativeness is priced.

Therefore, if more informative cybersecurity-related disclosures reduce investor uncertainty and improve the information environment, a negative association with the cost of equity should be expected on average. It also remains possible that the component dimensions of informativeness are not equally salient to investors, although the present study focuses on their aggregate effect through an overall CSRDS measure. Accordingly, although some disclosures may reveal greater underlying cyber exposure, the broader disclosure literature and the information-risk arguments reviewed above suggest that, on average, the net effect of higher overall CSRDS should remain negative because improved investor understanding reduces the uncertainty premium embedded in required return. Thus, this unresolved issue motivates the following hypothesis:

*H2: Higher cybersecurity-related disclosure informativeness is associated with a lower cost of equity.*

## **2.4 Literature Review for H3: Cross-country variation in the CSRDS-CoE relationship**

Prior literature indicates that the capital-market consequences of disclosure quality may vary across institutional environments (Bushman et al., 2004; Leuz & Wysocki, 2016). Building on H2, H3 examines whether the association between the informativeness of cybersecurity-related disclosure and the cost of equity differs between Australia and China. The following sections first clarify the comparative research gap and then develop the institutional channels through which the pricing consequences of CSRDS informativeness may vary across Australia and China.

### **2.4.1 Research gap and comparative motivation**

A substantial body of research suggests that more informative corporate disclosure is associated with lower information asymmetry and financing costs. These associations depend partly on the institutional environment in which disclosure is produced, interpreted, and incorporated into market prices (Hail, 2002; Richardson & Welker, 2001). More broadly, the disclosure literature indicates that firms adjust their reporting practices in response to transparency demands and capital-market pressures (Bushman et al., 2004; Leuz & Wysocki, 2016). Cybersecurity disclosure provides a distinctive setting because cyber risk is difficult for external investors to observe directly, increasing the potential importance of informative firm level narrative reporting (Amani et al., 2025; Liu & Babar, 2026). Recent review evidence indicates that although cybersecurity disclosure research has expanded rapidly, its capital-market implications have been examined primarily in the United States, while comparative and cross-country evidence remains limited (Amani et al., 2025).

Direct evidence on the capital-market pricing of CSRDS informativeness remains limited, and cross-country evidence is scarcer still. The closest direct evidence in the U.S. comes from Havakhor et al. (2026), which shows that disclosures of cybersecurity investments are associated with lower costs of accessing debt and equity capital, and that this effect is stronger when disclosures are more informative and analyst coverage is higher. Related U.S. evidence on disclosure mandates points in a broadly similar direction: Ashraf and Sunder (2023) and Elmawazini et al. (2023) both show that data breach disclosure regulations are associated with lower shareholder risk, proxied by the cost of equity. However, these studies examine disclosure mandates or investment-specific disclosure rather than a

multidimensional firm-level CSRDS informativeness construct. Comparative evidence is similarly limited. Barry et al. (2022) show that Chinese firms cross listed in the United States provide less cybersecurity disclosure than comparable U.S. domestic firms, but that the association between cybersecurity disclosure and firm valuation is stronger for the Chinese cross listed firms. Their findings suggest that institutional settings are associated with both disclosure practices and the market interpretation of disclosed information. Collectively, the available evidence indicates that cybersecurity disclosure has capital-market relevance and that its market implications may vary across institutional environments. It nevertheless remains unclear whether the association between CSRDS informativeness and the cost of equity differs across domestic reporting regimes. This study addresses that gap by comparing Australia and China, two settings that differ in enforcement architecture, investor composition, and the broader information environment.

#### **2.4.2 Institutional channels through which the CSRDS-CoE relation may vary across Australia and China.**

The same level of disclosure informativeness may be associated with different capital-market outcomes across institutional environments. This argument builds on H1 and H2. H1 predicts that CSRDS informativeness differs between Australia and China because disclosure is produced within different institutional environments. H2 predicts that more informative CSRDS is, on average, associated with a lower cost of equity because it may reduce information risk. H3 extends these arguments by asking whether the association between a given level of CSRDS informativeness and the cost of equity differs between the two countries. Three institutional channels may produce such variation. The first concerns whether investors regard disclosure as credible. The second concerns whether investors and information intermediaries can process the disclosed content and incorporate it into valuation. The third concerns whether annual report CSRDS provides incremental information beyond other available sources. These channels are related but conceptually distinct.

##### **2.4.2.1 Channel 1: Disclosure credibility**

The first channel concerns whether investors regard cybersecurity disclosure as credible. Informative CSRDS is more likely to be associated with a lower cost of equity when investors treat its content as a reliable signal of underlying cybersecurity preparedness and governance rather than as a formal

reporting exercise (Hail & Leuz, 2006; La Porta et al., 2006; Mercer, 2004). Credibility therefore depends not only on disclosure content but also on the institutional environment in which the disclosure is produced and interpreted. Cross-country research on investor protection, disclosure regulation, and private enforcement suggests that these conditions are associated with both disclosure quality and its capital-market implications (Hail & Leuz, 2006; La Porta et al., 1998, 2006). Differences between Australia and China therefore provide a basis for expecting the credibility channel to operate differently across the two countries.

The expected consequences of misleading or incomplete reporting may reinforce disclosure credibility. In Australia, ASIC can pursue civil penalties for breaches of continuous disclosure obligations, while investors may seek private remedies through securities class actions (ASIC, 2017; ASX, 2023; Australian Government, 2024). Empirical evidence also indicates that sanctions under Australia's continuous disclosure regime are associated with liquidity improvements for sanctioned firms and their industry peers (X. C. Chen et al., 2023). This evidence is consistent with investors having a stronger basis for treating detailed corporate disclosure as credible when misleading or incomplete reporting carries visible and enforceable consequences.

Enforcement of disclosure obligations in China operates through a more regulator led and hybrid institutional architecture. Broad institutional research characterises China's financial and legal system as less reliant on market driven private enforcement than common law systems, while more recent accounting and finance research shows that disclosure discipline remains strongly influenced by public and exchange based enforcement. Minority investor protection has increasingly been supplemented through state backed mechanisms, including the China Securities Investor Services Centre, and through reforms to private securities litigation (Allen et al., 2005; Cao et al., 2025; Y. Chen et al., 2021; Ke & Zhang, 2021; L. Li et al., 2024; Zhao et al., 2024). Nevertheless, this architecture remains less dependent on market driven private enforcement. Under these conditions, investors may perceive detailed voluntary disclosure as being less strongly supported by private enforcement consequences, potentially weakening the extent to which CSRDS is interpreted as a costly and credible signal of governance capability.

Holding informativeness constant, the credibility channel therefore predicts a stronger negative association between CSRDS informativeness and the cost of equity in Australia than in China. This expectation rests on differences in the expected consequences of misleading or incomplete reporting rather than on a simple distinction between investor facing and regulation oriented reporting systems.

#### **2.4.2.2 Channel 2: Investor processing and market uptake**

The second channel concerns whether market participants can process cybersecurity disclosure and incorporate it into valuation. This channel extends the H2 argument that informative disclosure is more likely to be reflected in financing outcomes when investors can interpret and use the information provided. Even when disclosure is credible, its association with the cost of equity may depend on whether investors and information intermediaries can interpret complex narrative content and translate it into assessments of risk and required return.

The Australian market may support this transmission mechanism through relatively stronger institutional intermediation and a more developed professional investment environment (ASIC, 2025; House of Representatives Standing Committee on Economics, 2022). Institutional investors, fund managers, and analysts are generally better positioned to interpret complex narrative disclosure, compare it across firms, and incorporate it into assessments of risk and required returns (Blankespoor et al., 2020; Kim & Ryu, 2022). This capacity is particularly relevant to cybersecurity reporting because informative disclosure often contains technical and qualitative discussion rather than simple numerical indicators. Such content may include governance arrangements, risk management processes, incident consequences, and mitigation activities (Amani et al., 2025; SEC, 2023). Where professional intermediation is stronger, this information is more likely to be interpreted and incorporated into market prices (Blankespoor et al., 2020; Huang et al., 2018; Kim & Ryu, 2022).

Australian and broader disclosure evidence is consistent with this interpretation. Shams et al. (2024) find that the extent of continuous disclosure by Australian bidders is positively associated with market reactions to merger and acquisition announcements, consistent with investors using such disclosure when assessing firm-specific transactions. Hope et al. (2016) similarly show that more specific risk factor disclosure is associated with stronger market reactions. These findings suggest that when

Australian firms provide specific and economically relevant CSRDS, market participants may be more likely to incorporate that information into valuation and required return assessments.

China may face comparatively greater processing frictions. Recent research characterises the Chinese equity market as relatively retail oriented, while active government participation remains an important feature of the market environment (Brunnermeier et al., 2022; Tan et al., 2024). In such a setting, complex narrative disclosure may be incorporated into prices less efficiently than in a market with deeper institutional intermediation. This issue is especially relevant to cybersecurity disclosure, which often contains technical language concerning internal controls, data protection, attack exposure, and remediation measures. Evidence relating to China's National Team intervention also indicates that government stock purchases are associated with reduced price informativeness, highlighting a potential tradeoff between market stabilisation and informational efficiency (Dang et al., 2024).

Broader disclosure research provides the theoretical basis for this argument. When information processing costs are high, firm-specific public information may be incorporated into prices less efficiently. Analysts and other intermediaries can mitigate these frictions by interpreting and disseminating complex disclosure (Blankespoor et al., 2020; Huang et al., 2018). Even when Chinese firms provide more informative CSRDS, market participants may therefore be less able to translate that improvement into a lower required return.

Holding CSRDS informativeness constant, the investor processing channel predicts a stronger negative association between CSRDS informativeness and the cost of equity in Australia than in China.

#### **2.4.2.3 Channel 3: Information environment and incremental value**

The third channel concerns whether annual report CSRDS provides incremental information beyond what investors can obtain from other sources. This channel is distinct from investor processing capacity. Strong professional intermediation may improve the interpretation of annual report disclosure while simultaneously reducing its incremental value because analysts, institutional investors, and financial media generate substitute information outside the annual reporting process.

Prior literature suggests that the pricing relevance of any individual disclosure depends on the surrounding information set. In stronger information environments, substitute information channels are more widely available. In weaker information environments, the same disclosure may provide greater incremental value because investors have fewer alternative sources of firm-specific information (Lang et al., 2012; Leuz & Wysocki, 2016). Krueger et al. (2024) provide related cross-country evidence by finding that firms in weaker information environments experience greater liquidity improvements following mandatory ESG disclosure. Although their study examines ESG rather than cybersecurity reporting, the underlying implication is similar: informative disclosure may have greater market relevance when substitute information sources are limited.

Two aspects may influence this channel in Australia and China. The first is the role of information intermediaries. Annual reports form only one component of a broader information environment in which analysts, institutional investors, financial media, and other intermediaries generate, interpret, and disseminate firm-specific information (Beyer et al., 2010; Healy & Palepu, 2001). In Australia, this intermediary based environment may reduce the incremental value of annual report CSRDS because cybersecurity information may already be interpreted, discussed, or partially incorporated into prices through analyst commentary, media coverage, institutional investor analysis, and other public channels.

By comparison, prior research characterises the Chinese equity market as more retail oriented and more strongly influenced by government participation (Tan et al., 2024). Where professional intermediation is thinner or varies substantially across firms, investors may have fewer alternative channels through which firm-specific cybersecurity information is interpreted and disseminated. On this dimension, annual report CSRDS may therefore provide lower incremental value in Australia but greater incremental value in China.

The second aspect concerns disclosure frequency and timeliness. The value of a particular reporting document depends partly on the quantity and timeliness of firm-specific information already available through other public channels (Beyer et al., 2010; Healy & Palepu, 2001; Leuz & Wysocki, 2016). Australia appears to provide a more continuous and timely public information environment. Under

ASX Listing Rule 3.1, listed entities must disclose market sensitive information immediately upon becoming aware of it, subject to limited exceptions (ASX, 2024). China's disclosure framework also imposes timeliness requirements, but the CSRC's 2021 Measures define timely disclosure as completion within two trading days of the relevant triggering point (CSRC, 2021a, Art. 62(3)).

This difference suggests that Australian investors may receive firm-specific updates outside the annual reporting cycle through a more continuous flow of public disclosure. Australian evidence also indicates that periodic earnings announcements and public information driven price movements constitute value relevant information events (Patel & Michayluk, 2016; Taylor & Tong, 2023). Greater disclosure timeliness may therefore reduce the incremental contribution of annual report CSRDS in Australia. By contrast, the less immediate disclosure window in China may leave the annual report with greater incremental value as a consolidated source of firm-specific cybersecurity information.

Evidence from China is broadly consistent with this incremental information argument. Wu et al. (2025) find that the capital-market consequences of cybersecurity disclosure are more pronounced among firms with lower analyst coverage, consistent with disclosure having greater importance when substitute information channels are limited. Other Chinese evidence shows that improvements in firm level disclosure quality and pricing efficiency are associated with a lower cost of equity (Q. Li et al., 2024; Yang et al., 2023). Although these studies do not directly examine CSRDS informativeness, they suggest that firm level public disclosure may have particular importance where alternative information channels are less developed.

Holding CSRDS informativeness constant, this channel alone may predict a stronger negative association between CSRDS informativeness and the cost of equity in China than in Australia. Annual report CSRDS may provide greater incremental firm-specific information when substitute public channels are limited. Unlike the credibility and investor processing channels, the information environment channel therefore introduces a competing prediction into H3 rather than reinforcing the same directional expectation.

### 2.4.3 Synthesis and Hypothesis Development

**Table 2.3**

*Summary of Institutional Channels and Predicted Effects*

| Channel                                       | Core idea                                                                                                                                                                                | Predicted stronger pricing effect |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Disclosure credibility                        | Informative CSRDS is more likely to affect the cost of equity when investors view it as a credible firm-specific signal rather than as formal compliance language                        | Australia                         |
| Investor processing and market uptake         | Informative CSRDS is more likely to be reflected in pricing when investors and information intermediaries can interpret and incorporate complex cyber-related disclosure into valuation. | Australia                         |
| Information environment and incremental value | The pricing value of annual-report CSRDS depends on whether it provides incremental information beyond other available public channels.                                                  | Potentially stronger in China     |

In conclusion, the preceding discussion suggests that the cost-of-equity effect developed in H2 should not be assumed to operate uniformly across institutional settings (Francis et al., 2005; Hail & Leuz, 2006; Leuz & Wysocki, 2016). More informative CSRDS is more likely to reduce financing costs when investors regard the disclosure as credible, when market participants can process the information, and when the disclosure provides incremental information beyond other available channels (Mercer, 2004; Blankespoor et al., 2020; Lang et al., 2012). The first two channels point more clearly toward Australia. In the Australian setting, the more visible expected consequences of misleading or incomplete disclosure provide stronger support for the credibility of detailed CSRDS, while stronger professional intermediation increases the likelihood that complex cyber-related information is processed and incorporated into valuation (Mercer, 2004; Blankespoor et al., 2020; Huang et al., 2018). The third channel, however, introduces a competing prediction. Because annual-report CSRDS may provide more incremental information where substitute public information channels are thinner, this channel may point toward a stronger pricing effect in China (Lang et al., 2012; Krueger et al., 2024). Overall, this study treats credibility and investor processing as primary transmission conditions for disclosure to affect required returns. Accordingly, although the information-environment channel suggests a possible countervailing effect, the overall expectation is:

*H3: The negative association between the informativeness of cybersecurity-related disclosure and cost of equity is stronger for Australian-listed firms than for Chinese-listed firms.*

## Chapter 3. Methodology and Data Collection

### 3.1 Overall Research Design

This study uses a quantitative archival research design to examine the informativeness of cybersecurity-related disclosure and its capital-market implications in Australia and Mainland China from FY2022 to FY2024. The empirical design first constructs firm-year measures of cybersecurity disclosure informativeness using Python-assisted content analysis of annual reports, consistent with the broader use of textual analysis in accounting and finance research (F. Li, 2010; Loughran & McDonald, 2016). The resulting Cybersecurity-Related Disclosure Score (CSRDS) measures are then combined with firm-year cost of equity data and control variables. The empirical analysis examines whether Australian firms provide more informative cybersecurity-related disclosure than Chinese firms, whether disclosure informativeness is associated with the cost of equity, and whether this association differs between the two countries. The main regression models are estimated using pooled OLS with fiscal-year fixed effects and firm-clustered standard errors, consistent with the broader disclosure and cost of capital literature (Botosan, 1997; Hail & Leuz, 2006).

CSRDS construction begins with a bilingual keyword and anchor-based procedure implemented in Python to identify potentially relevant cybersecurity passages in annual reports published in English and Chinese. The extracted passages are evaluated using the CSRDS codebook and scoring framework developed for this study. The framework measures disclosure informativeness across three dimensions: Specificity, Relevance, and Usefulness. These dimensions are operationalised through nine indicators, each scored on a three-point ordinal scale ranging from 0 to 2. The codebook-based approach is consistent with established content analysis methodology, which emphasises the systematic, transparent, and replicable coding of textual material (Krippendorff, 2019; Neuendorf, 2017).

The scoring criteria are implemented through machine-readable Python rules derived from the final codebook. Manual review is used to calibrate the rules and validate selected cases requiring greater interpretive judgement rather than to replace the rule-based scoring process for each firm-year observation. This combination of rule-based scoring and targeted human review improves consistency, transparency, and reproducibility while recognising that cybersecurity disclosure informativeness cannot be captured through raw keyword frequency alone (Loughran & McDonald, 2016).

For the empirical tests, the validated CSRDS measures are combined with firm-year financial and market data. The main dependent variable is the CAPM-based cost of equity. The models examine CSRDS at the aggregate, dimension, and indicator levels and test whether its associations with the cost of equity differ between Australia and China. This design integrates structured disclosure measurement with capital-market analysis. The CSRDS construction process translates annual report content into codebook-aligned measures of informativeness, while the regression analysis examines whether those measures are associated with firms' equity financing costs.

## **3.2 Sample Selection and Data Sources**

### **3.2.1 Country and Period Selection**

This study focuses on listed firms in Australia and China over three fiscal years: FY2022, FY2023 and FY2024. Australia and Mainland China are selected because they provide contrasting institutional settings for examining H1 and H3, as developed in Chapter 2. The sample period is selected to capture recent cybersecurity-related reporting practices during a period of heightened attention to cybersecurity risk, data protection, cyber governance and corporate cyber resilience. Recent research on cybersecurity disclosures also indicates that cybersecurity disclosure has become an expanding area of corporate reporting research, with studies increasingly focusing on disclosure characteristics, determinants, and outcomes (Amani et al., 2025).

The three-year period provides a recent and balanced firm-year panel while remaining feasible for detailed annual-report extraction, codebook-aligned scoring and validation. Using FY2022 to FY2024 also allows the study to examine cybersecurity-related disclosure informativeness across consecutive reporting periods rather than relying on a single-year cross-section.

### **3.2.2 Original Eligible Pool and Industry Restriction**

The sample was constructed from an industry-restricted eligible pool downloaded directly from the LSEG Workspace. Before firm-level sampling was conducted, the study first identified cyber-relevant industries based on Sustainability Accounting Standards Board (SASB) disclosure topics (IFRS Foundation, 2024). Industries were considered cyber-relevant where the SASB Standards identify disclosure topics related to data security, customer privacy, patient privacy, electronic health records,

or other information-system risks. This SASB-based review provided the conceptual rationale for focusing on industries in which cybersecurity-related disclosure is more likely to be economically meaningful to investors (SASB, 2017).

This industry rationale was then operationalised in LSEG by directly extracting listed firms from three relevant broad industry groups: Financials, Technology, and Healthcare. These industries were selected because firms in these sectors tend to rely heavily on digital infrastructure, customer or patient data, payment and transaction systems, regulated information systems, or technology-enabled business processes. Cybersecurity-related risks in these industries are therefore more likely to affect business operations, regulatory exposure, customer relationships and investor assessment.

The resulting LSEG industry-restricted eligible pool contained 166 Australian firms and 1,619 Chinese firms. In Australia, the eligible pool consisted of 96 firms in the Financial sector, 39 firms in the Technology sector, and 31 firms in the Healthcare sector. In China, the eligible pool comprised 144 firms in the Financial sector, 992 in the Technology sector, and 483 in the Healthcare sector. This pool formed the fixed candidate population from which the working and final samples were constructed.

To select the firm sample, a computer-assisted random ordering procedure was applied within each country-specific eligible pool. An initial buffer sample of 120 candidate firms was drawn for each country because the final sample required complete annual reports and regression data for the study period. Each candidate firm was then screened for the availability of annual reports, cost-of-equity data, control-variable data. Firms with incomplete or unsuitable data were excluded, and where necessary, replacement firms were selected from the same country-specific eligible pool using the same procedure. The final locked sample retained 100 eligible firms in each country with complete annual reports and regression data. This process ensured that all selected and replacement firms came from the same predefined eligible pool and were subject to the same sampling and screening rules.

The target of 100 firms per country reflects a research-design trade-off between cross-country comparability and sample breadth. Equal country allocation gives the two institutional settings comparable representation in the cross-country analyses and prevents the much larger Chinese eligible population from mechanically dominating the pooled sample. Although parts of the

evidence-extraction and scoring process were Python-assisted, constructing the 600 firm-year dataset still required substantial annual-report collection, processing, checking, and human validation in applying the nine-indicator disclosure measure across three reporting years.

The final Australian sample consists of 45 firms in the Financial sector, 28 firms in the Technology sector, and 27 firms in the Healthcare sector, while the Chinese sample consists of 6 firms in the Financial sector, 65 firms in the Technology sector, and 29 firms in the Healthcare sector.

Additional details on the industry composition of the original eligible pool and final locked sample are reported in Appendix 3A, Table 3A.1. The final sample firms, RICs, industry classifications, and fiscal years included are listed in Appendix 3A, Table 3A.2.

Each retained firm contributes annual report observations for FY2022, FY2023, and FY2024. Therefore, the final CSRDS scoring sample comprises 600 firm-year observations, including 300 Australian firm-years and 300 Chinese firm-years. The main regression sample also contains 600 firm-year observations because the final sample is restricted to firms with the annual-report, cost-of-equity and control-variable data required for the main analysis.

### 3.2.3 Data Sources

This study uses annual reports, market data and accounting data from several sources. Annual reports are hand-collected from official firm websites and official disclosure platforms, and they are used as the sole textual source for constructing CSRDS. The industry-restricted eligible pool, firm-level beta, accounting variables and market variables are obtained from LSEG Workspace (London Stock Exchange Group, n.d.). Country-year risk-free rates are obtained from LSEG Workspace, while country-year equity risk premia are obtained from Damodaran's country risk premium datasets; these inputs are used to construct the CAPM-based cost of equity (Damodaran, 2022, 2023, 2024; Lintner, 1965; Sharpe, 1964). The final dataset combines the CSRDS scores constructed from annual reports with the cost-of-equity and control-variable data required for the main regression analysis.

**Table 3.1**

*Sample Construction, Screening, and Replacement Process*

| Step                                                 | Australia | China | Total | Notes                              |
|------------------------------------------------------|-----------|-------|-------|------------------------------------|
| Firms in original eligible pool from LSEG extraction | 166       | 1,619 | 1,785 | Industry-restricted candidate pool |

|                            |     |     |     |                                                |
|----------------------------|-----|-----|-----|------------------------------------------------|
| Initial working sample     | 120 | 120 | 240 | First-round working sample                     |
| Final locked firm sample   | 100 | 100 | 200 | Firms retained after screening and replacement |
| FY2022 annual reports      | 100 | 100 | 200 | Included in CSRDS scoring                      |
| FY2023 annual reports      | 100 | 100 | 200 | Included in CSRDS scoring                      |
| FY2024 annual reports      | 100 | 100 | 200 | Included in CSRDS scoring                      |
| Final CSRDS scoring sample | 300 | 300 | 600 | Firm-year observations                         |
| Main regression sample     | 300 | 300 | 600 | Full main analysis sample                      |

*Note.* Firm-year observations are used in the main regression analysis.

### 3.3 Measurements of CSRDS

This section explains the construction of the Cybersecurity-Related Disclosure Score (CSRDS) for each firm-year in the 600-observation panel, and presents the measurement workflow in six components: the disclosure source and unit of analysis (Section 3.3.1), the CSRDS codebook and scoring framework (Section 3.3.2), the bilingual keyword dictionary (Section 3.3.3), the Python-based evidence-extraction procedure (Section 3.3.4), the refined Python scoring rules and calibration process (Section 3.3.5), and the post-refinement validation, reliability assessment, and final CSRDS construction (Section 3.3.6).

#### 3.3.1 Disclosure Source and Unit of Analysis

CSRDS construction measures the informativeness of cybersecurity-related disclosures using only annual reports. The annual report is treated as the relevant disclosure document because it provides the most standardised and comparable narrative reporting source across Australian and Chinese listed firms in the study sample. Candidate disclosure passages are first identified at the page and text-snippet level, but the final coding unit is the firm-year (Krippendorff, 2019; Neuendorf, 2017). In other words, extracted passages serve as evidence inputs, while final CSRDS scores are assigned at the firm-year level.

The annual report is selected as the single disclosure source for three reasons. First, in both jurisdictions, annual reports are formal, recurring documents that consolidate governance, risk, and operational information into a common reporting format, ensuring within-firm comparability. Second, stand-alone incident announcements and regulatory incident reports are event-driven and unbalanced across firms, which would bias any pooled disclosure-quality measure toward firms that experience or report specific cyber incidents. Third, prior cross-country disclosure-informativeness research consistently uses the annual report as the unit of analysis, supporting comparability with the literature (Botosan, 1997; Beretta & Bozzolan, 2008). The unit of analysis throughout CSRDS construction is

therefore the firm-year ( $n = 600$ ), with the PDF version of the annual report as the textual artefact.

### **3.3.2 CSRDS Codebook and Scoring Framework**

To evaluate the informativeness of cybersecurity-related disclosure, this study develops and applies a codebook and scoring framework to construct the Cybersecurity-Related Disclosure Score (CSRDS). This framework includes three dimensions: Specificity, Relevance and Usefulness. Specificity refers to the extent to which disclosure names concrete cyber threats, resilience mechanisms and assets rather than relying on boilerplate language. Relevance evaluates the degree to which disclosure connects cyber risk to firm-specific governance, business processes, and ecosystem/compliance context; and Usefulness refers to whether disclosure provides decision-useful quantification of inputs, exposures, or operational outcomes. This three-dimensional decomposition follows the broader disclosure-informativeness and disclosure-quality logic outlined in prior disclosure research and is adapted to the cybersecurity domain (Beretta & Bozzolan, 2008; Hope, 2003b; Barry et al., 2022; Amani et al., 2025). To maintain conceptual balance across dimensions and avoid over-weighting any single sub-theme, each dimension is operationalised through three indicators. The nine indicators are: S1 Specific cyber threats, S2 Cyber resilience and readiness, and S3 Cyber risks to key assets under Specificity; R1 Active cyber governance, R2 Cyber risk and business consequences, and R3 Third-party and compliance cyber risks under Relevance; and U1 Quantified cybersecurity resources, U2 Cyber insurance and exposure, and U3 Cybersecurity performance metrics under Usefulness. The detailed indicator definitions and typical annual-report sections used to guide evidence identification are provided in Appendix 3B, Table 3B.1.

The nine indicators are complementary components of a multidimensional construct of disclosure informativeness, not interchangeable predictors of a single economic outcome. Each captures a predefined attribute related to specificity, relevance, or usefulness of cybersecurity-related disclosure. They are combined to summarise the breadth and intensity of these attributes, without assuming that all nine share identical associations with capital-market outcomes.

Equal weighting is adopted *ex ante* to preserve conceptual symmetry across the nine indicators and to avoid outcome-driven weights based on subsequently observed statistical associations. The aggregate CSRDS score is therefore a transparent summary of the multidimensional construct, not an optimally

weighted predictor of the cost of equity. Aggregation inevitably trades indicator-level detail for construct-level parsimony and may obscure differences in the direction or magnitude of the economic associations of the underlying attributes. The empirical analysis therefore reports CSRDS at the aggregate, dimension, and indicator levels.

Each indicator is scored on a 0-2 ordinal scale. A score of 0 indicates that no evidence meets the minimum threshold for the relevant indicator. This may reflect either the absence of relevant disclosure or the presence of cybersecurity-related text that remains below the indicator threshold, a score of 1 indicates basic or general indicator-relevant disclosure, and a score of 2 indicates disclosure that satisfies the indicator-specific informative anchor, such as a named threat family for S1, a specific testing or readiness mechanism accompanied by qualifying evidence such as frequency, independent assessment, a measurable target, or a test outcome for S2. This bounded ordinal scale follows prior disclosure-quality research that uses structured scoring to distinguish disclosure quality from disclosure quantity (Botosan, 1997; Beretta & Bozzolan, 2008) and the bounded scale supports consistent comparison across indicators, firms, countries, and fiscal years. The full scoring criteria and evidence requirements for each indicator are reported in Appendix 3B, Table 3B.2.

**Table 3.2***The CSRDS Codebook: Nine Indicators × Three-Level Ordinal Scale*

| Dimension   | Code | Indicator                              | What it captures                                                                                      | Score 1: generic disclosure                                                                                                                                                           | Score 2: more informative disclosure                                                                                                                                                                                                      |
|-------------|------|----------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Specificity | S1   | Specific cyber threats                 | Whether the firm names concrete cyber threat types or attack vectors.                                 | Generic cyber-risk labels such as hacking, virus, or cyber-attack.                                                                                                                    | Identifiable cyber threat family/vector, such as ransomware, phishing, DDoS, supply-chain attack, APT, or zero-day exploit.                                                                                                               |
| Specificity | S2   | Cyber resilience and readiness         | Whether the firm describes specific cyber testing, monitoring, response, or resilience mechanisms.    | Generic mention of incident response plans, monitoring, or business continuity.                                                                                                       | Specific testing, monitoring, response, or resilience mechanisms accompanied by at least one qualifying detail, such as testing frequency, independent or third-party assessment, a measurable target such as RTO/RPO, or a test outcome. |
| Specificity | S3   | Cyber risks to key assets              | Whether cyber risk is linked to specific core systems, data, or digital assets.                       | Broad assets such as customer data or online services, without specific core asset identification.                                                                                    | Named core assets such as payment systems, trading systems, biometric databases, intellectual property, core algorithms, or critical information infrastructure, with explanation of their importance.                                    |
| Relevance   | R1   | Active cyber governance                | Whether cyber governance is active, accountable, and specific rather than merely structural.          | Static governance structure, such as audit committee oversight, without cyber-specific action.                                                                                        | Dynamic signals such as CISO reporting, board cyber expertise, cyber KPIs, accountability mechanisms, or reporting cadence.                                                                                                               |
| Relevance   | R2   | Cyber risk and business consequences   | Whether cyber risk is linked to operational or financial consequences through business processes.     | An identifiable operational, financial, regulatory, customer, reputational, or continuity consequence is stated, but no specific transmission mechanism/business process is explained | A specific business process/value-chain link is identified together with concrete consequence/transmission logic                                                                                                                          |
| Relevance   | R3   | Third-party and compliance cyber risks | Whether the firm discloses cyber-related third-party, supplier, compliance, or certification details. | Generic compliance statements with no standard, level, or mechanism.                                                                                                                  | Specific supplier assurance, audits, outsourcing controls, ISO 27001, SOC report, MLPS/等保 level, or other named cyber standards with scope or detail.                                                                                     |
| Usefulness  | U1   | Quantified cybersecurity resources     | Whether the firm quantifies cyber-related resources or defensive inputs.                              | Vague or partial quantification of cyber-specific resources, such as a percentage change without an interpretable base or amount.                                                     | Concrete cyber-specific resource figures, such as budget, headcount, training volume, or investment amount, together with a relevant timeframe.                                                                                           |
| Usefulness  | U2   | Cyber insurance and exposure           | Whether the firm discloses cyber risk transfer or downside exposure.                                  | Mentions cyber insurance without coverage details.                                                                                                                                    | Discloses insurance limits, deductibles, coverage scope, maximum probable loss, or quantified exposure.                                                                                                                                   |
| Usefulness  | U3   | Cybersecurity performance metrics      | Whether the firm provides measurable cybersecurity performance or assurance outcomes.                 | Generic statements such as stable operations or no major issue.                                                                                                                       | Specific KPIs or outcomes, such as MTTR, patching rate, vulnerability remediation, blocked attacks, uptime, audit results, or zero material incidents with clear security linkage.                                                        |

The aggregate CSRDS is calculated as the unweighted sum of the nine indicator scores. Each indicator therefore contributes equally to the aggregate score, consistent with the ex ante measurement design described above.

### **3.3.3 Bilingual Keyword Dictionary**

The study constructs a bilingual keyword dictionary directly from the CSRDS codebook to support evidence identification. The dictionary does not measure informativeness on its own (Loughran & McDonald, 2016). Instead, it serves as a retrieval tool for locating potentially relevant disclosure evidence for subsequent codebook-aligned scoring and manual review. The keyword system includes indicator-level keywords together with a separate set of cybersecurity anchor terms that constrain extraction to cybersecurity-relevant contexts. This rule-based design improves precision by reducing the risk of misclassifying generic discussions of technology, governance, or operational risk as cybersecurity-related disclosures.

The keyword dictionary is conceptually derived from the CSRDS framework rather than developed independently of it (Krippendorff, 2019; Neuendorf, 2017). In practical terms, the codebook determines the substantive content that should count as potentially relevant disclosure, and the keyword system is then designed to identify text segments that may contain that content. This ordering is important because it ensures that text extraction remains subordinate to the disclosure construct, rather than allowing keyword frequency to define the construct itself.

The development of the dictionary proceeds in several steps. For each CSRDS indicator, the study first identifies the core concepts that firms would typically discuss when providing relevant disclosure. Candidate keywords are then generated from three complementary sources: authoritative cybersecurity frameworks and standards such as the NIST Cybersecurity Framework and ISO/IEC 27001 (International Organization for Standardization, 2022; National Institute of Standards and Technology, 2024); regulatory and supervisory language describing cybersecurity risks and governance expectations; and wording from a pilot review of sample annual reports. Conceptually equivalent English and Chinese vocabulary lists are then developed on the basis of functional equivalence rather than literal translation, recognising that disclosure terminology may differ across reporting environments.

This approach establishes a transparent link between the conceptual definition of CSRDS and the evidence identification stage. Accordingly, the keyword dictionary is used to improve the efficiency and consistency of evidence retrieval, while the codebook remains the basis for substantive scoring. The bilingual keyword dictionary and cybersecurity anchor terms used for evidence retrieval are summarised in Appendix 3B, Table 3B.3.

### **3.3.4 Python-Based Evidence Extraction**

After the bilingual keyword dictionary was finalised, the annual report PDFs were processed using a Python-based evidence-extraction script. The script extracted text from each annual report at the page level and searched for cybersecurity-relevant passages using a combination of cybersecurity anchor terms and indicator-level keywords, consistent with the use of computer-assisted textual analysis in accounting and finance research (F. Li, 2010; Loughran & McDonald, 2016). The use of anchor terms was intended to reduce false positives by requiring extracted passages to occur in a cybersecurity-related context rather than in general discussions of technology, governance, business continuity or operational risk.

The extraction procedure was deliberately designed to be broader than the final scoring procedure. Its purpose was to identify candidate evidence for review and scoring, not to assign final CSRDS values. A text segment could therefore be extracted as potentially relevant evidence without necessarily receiving a positive CSRDS score. This distinction is important because the CSRDS framework measures disclosure informativeness, whereas the extraction procedure only locates potentially relevant text, consistent with content-analysis methodology that distinguishes evidence identification from substantive coding and interpretation (Krippendorff, 2019; Neuendorf, 2017).

The Python script exported the extracted evidence into a structured Evidence Review workbook. This workbook recorded the firm-year identifier, country, fiscal year, matched indicator, page reference, extracted text snippet and matching keyword evidence. It also produced indicator-specific sheets, a scoring summary sheet and a run log. These outputs created an auditable link between the original annual report text and the subsequent firm-year CSRDS scores.

The extraction process also included quality-assurance checks. Technical issues such as missing file

extensions, zero-hit observations not initially written to the scoring summary, and limitations in PDF text extraction were identified and resolved before the final scoring dataset was locked. These checks ensured that the final 600 firm-year scoring sample was complete before the refined scoring rules were applied.

### **3.3.5 Refined Python Scoring and Rule Calibration**

After evidence extraction, the extracted passages were scored using a Python-based rule system derived from the CSRDS codebook. Each 0–2 indicator threshold in the codebook was translated into machine-readable decision logic to support consistent application of the scoring criteria across the 600 firm-year observations.

Manual review was used at this stage as a calibration tool rather than as a full manual scoring procedure. A set of manually reviewed cases was used to identify where the initial rule logic misclassified disclosure evidence. The recurring issues were specific: false positives from product-only descriptions of cybersecurity, false positives from non-cyber emergency or business-continuity language, generic governance terms that did not establish cyber-specific accountability, and boundary cases between level 1 and level 2 disclosure. The scoring rules were then revised to address these patterns, and the scoring procedure was rerun across the full sample.

The refined scoring logic used a two-layer structure. A passage had to include cybersecurity-related anchor terms and indicator-specific evidence to receive a positive score. Evidence was also classified by confidence level. Stronger, more direct matches were treated as candidates for automated acceptance, while weaker or more judgement-intensive cases were flagged for manual review. This structure was introduced to reduce false positives and to ensure that generic technology, risk-management or governance language did not automatically receive a CSRDS score.

This approach preserves the consistency of automated scoring while retaining a substantive link to the codebook: a positive score is assigned only when the extracted text satisfies the relevant indicator threshold. Following this calibration stage, the refined rules were applied to the full sample. A separate post-refinement validation step was then used to assess whether the resulting rule-based scores were consistent with structured manual application of the final codebook.

### 3.3.6 Post-Refinement Validation, Reliability Assessment and Final CSRDS Construction

After applying the refined Python scoring rules to the full 600 firm-year sample, this thesis conducted a stratified validation check before locking the final CSRDS dataset. The validation addressed one methodological question: whether the rule-based scores were consistent with those a human reviewer would assign using the same final codebook. This step was necessary because cybersecurity-related disclosure is judgement-sensitive. A passage may contain relevant terminology, such as technology, governance, operational risk or business continuity, but still fall short of the substantive threshold required by a CSRDS indicator.

The post-refinement validation sample comprised 36 firm-year observations, with six drawn from each country-year cell: six Australian and six Chinese observations for each of FY2022, FY2023, and FY2024. Within each cell, the selection procedure covered zero-, low-, medium-, and high-score observations and included higher-judgement indicator cases. Any remaining positions were filled randomly using a fixed random seed. This stratified approach ensured that the validation was not concentrated in a single part of the CSRDS distribution or limited to straightforward coding cases.

All annual reports for the Chinese observations, including the 18 Chinese firm-year observations in the validation sample, were Chinese-language documents. The validation directly assessed how the bilingual extraction and scoring procedure applied to original Chinese-language sources, rather than to translated English versions. Each selected firm-year was re-assessed against the final codebook across all nine CSRDS indicators, producing 324 paired rule-based and manual indicator-level decisions. Five indicator-level disagreements were identified and corrected before the final CSRDS dataset was locked.

Coding consistency was assessed using both raw percentage agreement and Cohen's kappa. Percentage agreement provides a direct measure of how often the rule-based score matched the human validation judgement. However, because percentage agreement does not adjust for chance agreement, Cohen's kappa was also calculated. Since the CSRDS indicators are ordinal (0-2), quadratic-weighted kappa is preferred. This weighting recognises that a disagreement between 0 and 2 is more serious than a disagreement between adjacent categories. This use of weighted kappa is consistent with Cohen's original logic of allowing scaled disagreement or partial credit for ordered coding categories.

Across the 324 paired indicator-level decisions, the rule-based scores and human validation judgement agreed on 319 decisions, producing a percentage agreement of 98.46%. The overall unweighted kappa was 0.969, and the overall quadratic-weighted kappa was 0.983. At the indicator level, quadratic-weighted kappa ranged from 0.879 for R1 to 1.000 for indicators with complete agreement. These results indicate a very high level of agreement between the codebook-aligned Python scoring rules and the human validation judgement. Table 3.3 summarises the reliability results, while the full indicator-level breakdown is reported in Appendix 3C, Table 3C.1.

These statistics reflect post-refinement coding consistency between the rule-based scoring procedure and structured manual re-judgement using the same codebook. The validation was not an independent blind double-coding exercise between two human coders. The researcher who developed and applied the scoring framework manually re-examined the 36 selected firm-year observations against the final codebook and the underlying annual-report evidence. The agreement and kappa statistics therefore provide evidence of consistency in applying the scoring framework, but they do not by themselves establish the construct validity of CSRDS, demonstrate that CSRDS captures all dimensions of investor-relevant disclosure informativeness, or show superiority over alternative disclosure measures.

**Table 3.3***Post-Refinement Validation Sample and Machine–Human Reliability**Panel A. Validation sample by country and fiscal year*

| Country      | 2022 | 2023 | 2024 | Total |
|--------------|------|------|------|-------|
| AU           | 6    | 6    | 6    | 18    |
| CN           | 6    | 6    | 6    | 18    |
| <b>Total</b> | 12   | 12   | 12   | 36    |

*Panel B. Validation sample by score bucket*

| Country      | high | low | medium | zero | Total |
|--------------|------|-----|--------|------|-------|
| AU           | 3    | 4   | 7      | 4    | 18    |
| CN           | 3    | 7   | 4      | 4    | 18    |
| <b>Total</b> | 6    | 11  | 11     | 8    | 36    |

*Panel C. Reliability summary*

| Sample      | Firm-year<br>N | Indicator decisions | Disagreements | Agreement % | Quadratic-weighted $\kappa$ | 95% CI           | Exact-match firm-years | Exact-match % |
|-------------|----------------|---------------------|---------------|-------------|-----------------------------|------------------|------------------------|---------------|
| Full sample | 36             | 324                 | 5             | 98.46       | 0.9825                      | [0.9648, 0.9965] | 32                     | 88.89         |
| Australia   | 18             | 162                 | 4             | 97.53       | 0.9744                      | [0.9482, 1.0000] | 15                     | 83.33         |
| China       | 18             | 162                 | 1             | 99.38       | 0.9923                      | [0.9721, 1.0000] | 17                     | 94.44         |

Note. The validation sample contains six firm-year observations from each country-year cell. Score-bucket labels correspond to the categories used in the post-refinement validation procedure. Agreement is calculated across the nine indicator decisions for each firm-year. Quadratic-weighted Cohen’s kappa is reported as the primary reliability coefficient because indicator scores are ordinal (0–2). Kappa confidence intervals are percentile 95% intervals from 10,000 bootstrap replications that resample firm-year observations and retain all nine indicator decisions within each selected firm-year. The manual review was a structured codebook re-judgement of the automated scores, not an independent blind double-coding exercise. Agreement and kappa therefore assess coding consistency and do not, by themselves, establish construct validity.

After validation, the CSRDS dataset was locked and used for all descriptive and regression analyses. Scores are retained in raw form. Each indicator ranges from 0 to 2. Each dimension score is calculated as the sum of its three constituent indicators and ranges from 0 to 6. The aggregate CSRDS\_Total score is the sum of all nine indicators and ranges from 0 to 18. This raw scoring structure is retained because it directly corresponds to the codebook and avoids the interpretive ambiguity that arises when converting scores to a percentage index.

### 3.4 Economic Consequence Tests

#### 3.4.1 Construction of the Regression Dataset

The regression dataset combines the final validated CSRDS scores with the firm-year financial and market variables required for the empirical tests. The dataset is constructed at the firm-year level and contains 600 observations, corresponding to 100 Australian firms and 100 Chinese firms observed over FY2022, FY2023 and FY2024. It includes CSRDS measures at the aggregate, dimension and indicator-levels, the cost-of-equity measure, and the firm-level control variables described in Section 3.4.3.

#### 3.4.2 Dependent Variable: Cost of Equity

The main dependent variable is the CAPM-based cost of equity. The CAPM is used because it provides a transparent and theoretically grounded estimate of the required return on equity based on systematic risk. The study does not independently estimate firm beta. Instead, firm level beta is measured using the five year monthly beta obtained from LSEG Workspace and used as an input in the CAPM based cost of equity calculation. For each firm-year observation, the CAPM-based cost of equity is calculated as follows:

$$CoE_{i,t} = Rf_{c,t} + \beta_{i,t} \times ERP_{c,t} \quad (3.1)$$

where  $CoE_{i,t}$  is the cost of equity for firm  $i$  in fiscal year  $t$ , and  $Rf_{c,t}$  is risk free rate for country  $c$  in fiscal year  $t$ , and  $\beta_{i,t}$  is the firm-level beta and  $ERP_{c,t}$  is the equity risk premium for country.

The country-year risk-free rate is measured using country-specific three-year government bond yields obtained from LSEG Workspace, specifically AU3YT=RR for Australia and CN3YT=RR for China. Firm-level beta is measured using LSEG's five-year monthly beta. The country-year equity risk

premium is measured using the total equity risk premium from Damodaran's country risk premium datasets for 2022, 2023 and 2024 (Damodaran, 2022, 2023, 2024). The total equity risk premium is used rather than the country risk premium alone because the CAPM calculation requires the full market equity risk premium.

### **3.4.3 Control Variables**

The regression models include nine firm-level controls and an Australia country indicator. These controls are selected from prior disclosure, information-risk and cost-of-equity research to account for firm fundamentals, capital structure, profitability, earnings risk, information environment, liquidity, valuation differences and firm maturity.

Firm size is measured as the natural logarithm of total assets. Larger firms often have more developed information environments and may face different equity financing costs (Botosan, 1997; Hail & Leuz, 2006). Leverage is measured as total liabilities divided by total assets and controls for differences in financial risk. Return on assets is measured as net income divided by total assets and controls for profitability and operating performance (Dhaliwal et al., 2011; Francis et al., 2004). Earnings volatility is measured as the standard deviation of ROA over the available observation period for each firm and captures instability in accounting performance and earnings related risk (Francis et al., 2004).

Analyst coverage is measured as  $\ln(1+\text{number of analysts})$ . Analyst following reflects the firm's information environment and may reduce information asymmetry (Bowen et al., 2008; Easley & O'Hara, 2004; Lang & Lundholm, 1996). The loss dummy equals one when net income is negative and zero otherwise and controls for the different valuation characteristics of loss firms (Hayn, 1995).

Liquidity is measured as the natural logarithm of average daily trading volume. Trading activity is commonly used as a liquidity proxy, and liquidity is associated with expected returns and the cost of capital (Amihud, 2002; Chordia et al., 2001; Easley & O'Hara, 2004). Book to market is measured as the book value of equity divided by the market value of equity and controls for differences between value and growth firms that are associated with expected returns and implied cost of capital (Fama & French, 1992; Gebhardt et al., 2001). Listing age is measured at the firm-year level as  $\ln(1+\text{years since listing})$ . This variable controls for differences in firm maturity because younger listed firms may be

subject to greater uncertainty regarding profitability, valuation, and return volatility (Pástor & Veronesi, 2003).

The pooled models also include an Australia indicator, which equals one for Australian firm-year observations and zero for Chinese firm-year observations. China is therefore the reference country. The indicator controls for average differences between Australian and Chinese observations, including differences in regulation, market structure, and reporting environment that are not captured by the firm level controls. Fiscal year fixed effects are also included, with FY2022 serving as the omitted reference year and indicators included for FY2023 and FY2024. These fixed effects control for common time varying factors affecting all firms in a given fiscal year.

Detailed definitions and data sources for the regression variables are provided in Appendix 3D, Table 3D.1.

### 3.5 Empirical Models

Equation (3.1) defines the CAPM-based cost of equity used as the dependent variable in the H2 and H3 models. Equation (3.2) tests H1 using CSRDS as the dependent variable, while Equations (3.3) to (3.7) examine the association between CSRDS and the cost of equity. The CAPM equation is therefore a variable construction equation, whereas Equations (3.2) to (3.7) specify the empirical models used for hypothesis testing and supplementary analysis.

#### 3.5.1 H1 Model: Cross-Country CSRDS Comparison

H1 predicts that Australian firms provide more informative cybersecurity related disclosures than Chinese firms. The analysis first reports descriptive comparisons by country and fiscal year and conducts Welch two sample t tests. It then estimates the country difference model presented in Equation (3.2):

$$CSRDSMeasure_{i,t} = \alpha_0 + \alpha_1 AU_i + \sum_t \gamma_t Year_t + \varepsilon_{i,t} \quad (3.2)$$

In Equation (3.2),  $CSRDSMeasure_{i,t}$  denotes the aggregate CSRDS score, one of the three dimension scores, or one of the nine indicator scores for firm i in fiscal year t. A separate model is estimated for each CSRDS measure. The Australia indicator equals one for Australian firm-year observations and zero for Chinese firm-year observations, making China the reference group. Fiscal

year fixed effects control for common differences across FY2022, FY2023, and FY2024.

The coefficient on the Australia indicator represents the average difference between Australian and Chinese firm-year observations after controlling for fiscal year effects. A positive and statistically significant coefficient is consistent with H1. This coefficient is interpreted as an adjusted country difference rather than as a causal estimate of the effect of the institutional environment on disclosure informativeness.

### 3.5.2 H2 Model: Aggregate, Dimension, and Indicator-level Analyses

The aggregate CSRDS model provides the primary test of H2. H2 predicts that greater cybersecurity disclosure informativeness is associated with a lower cost of equity. Equation (3.3) estimates this association using the aggregate CSRDS score:

$$CoE_{i,t} = \beta_0 + \beta_1 CSRDS_{i,t} + \beta_2 AU_i + \sum_k \theta_k Control_{k,i,t} + \sum_t \gamma_t Year_t + \varepsilon_{i,t} \quad (3.3)$$

In Equation (3.3),  $CoE_{i,t}$  denotes the CAPM-based cost of equity,  $CSRDS_{i,t}$  denotes the aggregate cybersecurity disclosure score, and  $AU_i$  denotes the Australia indicator. The model also includes the firm level controls defined in Section 3.4.3 and fiscal year fixed effects. Standard errors are clustered by firm. H2 predicts a negative coefficient on aggregate CSRDS.

The dimension level analysis supplements the aggregate test by examining the three CSRDS dimensions jointly. Equation (3.4) replaces the aggregate CSRDS score with Specificity, Relevance, and Usefulness:

$$CoE_{i,t} = \beta_0 + \beta_1 Specificity_{i,t} + \beta_2 Relevance_{i,t} + \beta_3 Usefulness_{i,t} + \beta_4 AU_i + \sum_k \theta_k C_{k,i,t} + \sum_t \gamma_t Year_t + \varepsilon_{i,t} \quad (3.4)$$

The coefficients on Specificity, Relevance, and Usefulness represent the conditional association between each dimension and the cost of equity after accounting for the other two dimensions, the Australia indicator, the firm level controls, and fiscal year fixed effects. Because the dimensions are entered jointly, each coefficient is interpreted conditional on the other dimensions included in the model.

Equation (3.5) further disaggregates CSRDS by entering all nine indicators jointly. This specification

examines whether particular disclosure attributes have conditional associations with the cost of equity that may be obscured when the indicators are combined into dimension or aggregate scores:

$$\text{CoE}_{i,t} = \beta_0 + \sum_{j=1}^9 \beta_j \text{Indicator}_{i,t}^j + \beta_{10} \text{AU}_i + \sum_m \theta_m \text{Control}_{m,i,t} + \sum_t \gamma_t \text{Year}_t + \varepsilon_{i,t} \quad (3.5)$$

Each indicator coefficient represents its conditional association with the cost of equity after accounting for the other eight indicators, the Australia indicator, the firm level controls, and fiscal year fixed effects. To assess whether the indicator level results are sensitive to the simultaneous inclusion of the other indicators, Appendix 4A, Table 4A.2 reports supplementary models in which each indicator is entered separately. These models are treated as sensitivity analyses and do not replace the aggregate CSRDS model as the primary test of H2.

### 3.5.3 H3 Model: Cross-Country Difference in the Association between CSRDS and the Cost of Equity

H3 predicts that the negative association between CSRDS informativeness and the cost of equity is stronger in Australia than in China. The primary test of H3 uses the aggregate interaction model presented in Equation (3.6):

$$\text{CoE}_{i,t} = \beta_0 + \beta_1 \text{CSRDS}_{i,t} + \beta_2 \text{AU}_i + \beta_3 (\text{CSRDS}_{i,t} \times \text{AU}_i) + \sum_m \theta_m \text{Control}_{m,i,t} + \sum_t \gamma_t \text{Year}_t + \varepsilon_{i,t} \quad (3.6)$$

China is the reference group. The coefficient on CSRDS represents the association between aggregate CSRDS and the cost of equity for Chinese firm-year observations. The interaction coefficient represents the difference between the Australian and Chinese slopes. The total Australian slope is calculated as the sum of the CSRDS main effect and the interaction coefficient.

H3 predicts a negative and statistically significant interaction coefficient. The interaction term provides the formal test of whether the Australian association is more negative than the Chinese association. Differences in statistical significance between separately estimated country models do not, by themselves, establish a statistically significant difference between the two slopes.

A supplementary interaction model applies the same structure to R2, Cyber risk and business consequences. This analysis examines whether the R2 association with the cost of equity differs between Australia and China:

$$CoE_{i,t} = \beta_0 + \beta_1 Indicator_{i,t} + \beta_2 AU_i + \beta_3 (Indicator_{i,t} \times AU_i) + \sum_m \theta_m Control_{m,i,t} + \sum_t \gamma_t Year_t + \varepsilon_{i,t} \quad (3.7)$$

In this supplementary model, the R2 main effect represents the association between business consequence disclosure and the cost of equity for Chinese firm-year observations. The interaction coefficient represents the difference between the Australian and Chinese R2 slopes, while the total Australian slope is calculated as the sum of the R2 main effect and the interaction coefficient. A negative and statistically significant interaction coefficient would indicate that the R2 association is more negative in Australia than in China. This supplementary analysis does not replace the aggregate interaction model as the primary test of H3.

### 3.6 Robustness and Sensitivity Analyses

Several robustness and sensitivity analyses are conducted to assess whether the main inferences are sensitive to broad sector adjustment, alternative measurement choices, extreme observations, the treatment of zero and positive CSRDS scores, governance controls, and models estimated separately by country.

First, the H2 and H3 models are reestimated using LSEG StarMine Weighted Average Cost of Capital (WACC), obtained through LSEG Workspace, as an alternative market based financing cost outcome. LSEG StarMine WACC estimates the average rate a firm is expected to pay to providers of debt, common equity, and preferred equity, with each component weighted according to the firm's capital structure. Compared with the CAPM based cost of equity used in the main analysis, WACC provides a broader perspective on financing costs. This test assesses whether the main empirical patterns remain observable when a broader financing cost outcome is used in place of the CAPM based cost of equity.

Second, continuous variables were Winsorised at the 1st and 99th percentiles to assess whether the main results were driven by outliers in the cost-of-equity indicators or other continuous regression

variables. If the main findings remain similar after Winsorisation, this further confirms that these results are not overly sensitive to extreme values.

Third, aggregate CSRDS is replaced with a positive CSRDS indicator that equals one when at least one indicator receives a positive score and zero otherwise. This specification examines whether achieving a positive CSRDS score is associated with the cost of equity.

Fourth, the aggregate CSRDS and R2 models are reestimated using only firm-year observations with positive CSRDS scores. This restricted sample analysis examines whether variation in disclosure informativeness remains associated with the cost of equity after zero score observations are excluded.

Fifth, governance controls are added in the subsample for which board governance data are available. Board independence and board size serve as additional controls. This test examines whether the main disclosure results, particularly the indicator-level evidence, remain robust after controlling for observable governance characteristics. Because the governance-control test relies on a smaller subsample and captures only selected board attributes, it is best viewed as supplementary evidence rather than a definitive causal test.

Finally, separate models are estimated for the Australian and Chinese subsamples as supplementary sensitivity analyses. These models provide descriptive evidence on whether the association between CSRDS and the cost of equity is evident within each country. Because differences in statistical significance across subsamples do not necessarily imply a statistically significant difference in coefficients, cross-country moderation is assessed using the pooled interaction models described in Section 3.5.3.

As an additional robustness test for H1, Equation (3.2) is reestimated with broad sector fixed effects for Healthcare and Technology, with Financials serving as the reference sector. This specification controls for relatively stable observed and unobserved characteristics shared by firms within the same broad sector that may systematically affect cybersecurity disclosure informativeness. The sector adjusted specification is treated as supplementary robustness evidence and does not replace the baseline H1 model.

To address the materially different industry composition of the Australian and Chinese samples, the principal H2 and H3 specifications are re-estimated with broad industry fixed effects. Financials serves as the reference category, and indicators for Healthcare and Technology are added to the models. The industry-adjusted specifications include the aggregate H2 model, the jointly estimated CSRDS dimensions, the joint nine-indicator model, and the aggregate H3 interaction model. These analyses test whether the substantive H2 and H3 conclusions, particularly the R2 indicator-level result, are sensitive to systematic differences across the three sampled industries.

Because the indicator-level analysis examines multiple related CSRDS indicators in both joint and separate-indicator specifications, multiplicity-adjusted inference is also reported. The primary adjustment treats the nine coefficients from the joint indicator model and the corresponding nine separate-indicator coefficients as an 18-test family within each financing-cost outcome and industry-fixed-effects specification. Holm's sequential adjustment controls the family-wise error rate. Both unadjusted and Holm-adjusted p values are reported, with particular attention to whether the R2 result remains statistically significant after adjustment.

These analyses test whether the main inferences remain stable after broad industry adjustment in the H1, H2 and H3 specifications, when LSEG StarMine WACC is used as an alternative market-based financing-cost outcome, after winsorisation, under alternative treatments of zero and positive CSRDS observations, after the addition of governance controls, and when models are estimated separately by country. Multiplicity-adjusted inference is also used to assess whether the indicator-level R2 result is robust to the examination of multiple CSRDS indicators.

## Chapter 4. Results

The empirical results follow the model structure developed in Section 3.5. Equation (3.1) defines the CAPM-based cost of equity used as the primary dependent variable in the H2 and H3 analyses. Equation (3.2) specifies the country comparison model used to test H1. Equation (3.3) provides the primary test of H2, while Equations (3.4) and (3.5) report supplementary dimension and indicator-level analyses. Equation (3.6) provides the primary interaction test of H3, and Equation (3.7) reports the supplementary R<sup>2</sup> interaction analysis. To avoid repeating the equations in this chapter, each regression table refers to the corresponding model in Chapter 3. Unless otherwise stated, the H2 and H3 regressions include the Australia indicator, the firm level controls described in Section 3.4.3, fiscal year fixed effects, and standard errors clustered by firm.

### 4.1 Descriptive Statistics and Correlation Matrix

#### 4.1.1 Descriptive Statistics

Table 4.1 presents the descriptive statistics for the main cost-of-equity regression sample. The final sample consists of 600 firm-year observations, including 100 Australian and 100 Chinese firms, observed over the FY2022 to FY2024 reporting periods. The primary regression sample contains no missing values for the variables used in the main analyses, which includes disclosure scores, the cost of equity, and control variables. Panel A reports the pooled sample, while Panels B and C report the Australian and Chinese subsamples separately.

The descriptive statistics in Panel A show that overall cybersecurity-related disclosure informativeness is generally low in the pooled sample. The mean CSRDS score is 2.05 on a 0-18 scale, and the median is 1. This distribution indicates that cybersecurity disclosure informativeness is generally limited across the sample. The distribution is also right-skewed, as reflected in the low median and the interquartile range from 0 to 4. The low average score is partly driven by observations with zero scores. As shown in Table 4.2, 243 firm-year observations, or 40.5 per cent of the total sample, received a CSRDS score of zero. However, these zero score observations do not all have the same meaning. Of the 243 zero score observations, 137 contain no extracted cybersecurity related text, while 106 contain cyber related text that does not meet the minimum scoring threshold for any indicator. The low pooled

CSRDS score therefore reflects both the absence of extracted cyber related text and the presence of text below the scoring threshold. A zero score should not be interpreted uniformly as either disclosure absence or limited disclosure informativeness.

The cost of equity has a mean of 9.4 per cent and a median of 9.0 per cent, with an interquartile range of 7.4 per cent to 11.0 per cent. Panels B and C show that the mean cost of equity is higher for Australian firm-years than for Chinese firm-years. This descriptive difference reinforces the need to control for country and firm-level characteristics in the regression analysis.

The dimension-level statistics provide further context. According to Table 4.1, Specificity has the highest mean score among the three dimensions, which is 1.240, followed by Relevance, while Usefulness is very low across the sample. This indicates that firms are more likely to discuss specific threats, preparedness mechanisms, or critical assets than to provide quantified resources, cyber insurance details, or measurable incident outcomes.

Panels B and C report the same statistics separately for the Australian and Chinese subsamples. The two groups are similar in average size but differ on several characteristics that are relevant to the cost of equity. Australian firm-years have higher mean CSRDS scores than Chinese firm-years, and the same pattern holds across Specificity, Relevance, and Usefulness. However, the two subsamples also differ in several firm-level characteristics. Australian firms have higher analyst coverage, higher listing age, higher mean cost of equity, a higher incidence of loss years, and higher leverage, while Chinese firms have higher trading liquidity and higher average profitability. These differences justify the inclusion of firm-level controls and a country indicator in the subsequent regression models.

**Table 4.1***Descriptive Statistics*

| <b>Variable</b>                                          | <b>N</b> | <b>Mean</b> | <b>SD</b> | <b>Q1</b> | <b>Median</b> | <b>Q3</b> |
|----------------------------------------------------------|----------|-------------|-----------|-----------|---------------|-----------|
| <b><i>Panel A. Full sample</i></b>                       |          |             |           |           |               |           |
| CSRDS score                                              | 600      | 2.050       | 2.338     | 0.000     | 1.00          | 4.000     |
| Cost of equity                                           | 600      | 0.094       | 0.031     | 0.074     | 0.090         | 0.110     |
| Specificity                                              | 600      | 1.240       | 1.466     | 0.000     | 1.000         | 2.000     |
| Relevance                                                | 600      | 0.662       | 0.877     | 0.000     | 0.000         | 1.000     |
| Usefulness                                               | 600      | 0.148       | 0.443     | 0.000     | 0.000         | 0.000     |
| Firm size                                                | 600      | 20.617      | 1.745     | 19.584    | 20.449        | 21.551    |
| Leverage                                                 | 600      | 0.408       | 0.306     | 0.176     | 0.343         | 0.565     |
| ROA                                                      | 600      | 0.007       | 0.226     | 0.003     | 0.032         | 0.068     |
| Earnings volatility                                      | 600      | 0.055       | 0.098     | 0.009     | 0.023         | 0.050     |
| Analyst coverage                                         | 600      | 1.253       | 1.063     | 0.000     | 1.386         | 2.197     |
| Loss dummy                                               | 600      | 0.227       | 0.419     | 0.000     | 0.000         | 0.000     |
| Liquidity                                                | 600      | 16.059      | 1.898     | 14.846    | 16.320        | 17.280    |
| Book-to-market                                           | 600      | 0.475       | 0.473     | 0.189     | 0.331         | 0.573     |
| Listing age                                              | 600      | 2.390       | 0.847     | 1.792     | 2.565         | 3.045     |
| <b><i>Panel B. Australian firm-year observations</i></b> |          |             |           |           |               |           |
| Cost of equity                                           | 300      | 0.099       | 0.035     | 0.076     | 0.095         | 0.119     |
| CSRDS score                                              | 300      | 2.823       | 2.314     | 1.000     | 3.000         | 4.000     |
| Specificity                                              | 300      | 1.677       | 1.483     | 0.000     | 2.000         | 3.000     |
| Relevance                                                | 300      | 0.937       | 0.925     | 0.000     | 1.000         | 1.000     |
| Usefulness                                               | 300      | 0.210       | 0.517     | 0.000     | 0.000         | 0.000     |
| Firm size                                                | 300      | 20.541      | 2.045     | 19.253    | 20.388        | 21.730    |
| Leverage                                                 | 300      | 0.459       | 0.350     | 0.210     | 0.400         | 0.645     |
| ROA                                                      | 300      | -0.008      | 0.280     | -0.011    | 0.020         | 0.068     |
| Earnings volatility                                      | 300      | 0.065       | 0.102     | 0.009     | 0.025         | 0.067     |
| Analyst coverage                                         | 300      | 1.774       | 0.923     | 1.099     | 1.946         | 2.565     |
| Loss dummy                                               | 300      | 0.283       | 0.451     | 0.000     | 0.000         | 1.000     |
| Liquidity                                                | 300      | 14.887      | 1.789     | 13.472    | 14.862        | 16.005    |
| Book-to-market                                           | 300      | 0.533       | 0.553     | 0.153     | 0.350         | 0.741     |

| Variable                                              | N   | Mean   | SD    | Q1     | Median | Q3     |
|-------------------------------------------------------|-----|--------|-------|--------|--------|--------|
| Listing age                                           | 300 | 2.689  | 0.818 | 2.168  | 2.890  | 3.219  |
| <b><i>Panel C. Chinese firm-year observations</i></b> |     |        |       |        |        |        |
| Cost of equity                                        | 300 | 0.088  | 0.024 | 0.072  | 0.086  | 0.103  |
| CSRDS score                                           | 300 | 1.277  | 2.096 | 0.000  | 0.000  | 2.000  |
| Specificity                                           | 300 | 0.803  | 1.313 | 0.000  | 0.000  | 1.000  |
| Relevance                                             | 300 | 0.387  | 0.730 | 0.000  | 0.000  | 1.000  |
| Usefulness                                            | 300 | 0.087  | 0.346 | 0.000  | 0.000  | 0.000  |
| Firm size                                             | 300 | 20.694 | 1.381 | 19.822 | 20.464 | 21.271 |
| Leverage                                              | 300 | 0.356  | 0.246 | 0.165  | 0.286  | 0.507  |
| ROA                                                   | 300 | 0.022  | 0.153 | 0.010  | 0.038  | 0.068  |
| Earnings volatility                                   | 300 | 0.044  | 0.092 | 0.008  | 0.020  | 0.039  |
| Analyst coverage                                      | 300 | 0.731  | 0.932 | 0.000  | 0.000  | 1.386  |
| Loss dummy                                            | 300 | 0.170  | 0.376 | 0.000  | 0.000  | 0.000  |
| Liquidity                                             | 300 | 17.232 | 1.120 | 16.505 | 17.141 | 17.930 |
| Book-to-market                                        | 300 | 0.418  | 0.369 | 0.205  | 0.321  | 0.487  |
| Listing age                                           | 300 | 2.090  | 0.767 | 1.386  | 2.197  | 2.656  |

*Note.* This table reports descriptive statistics for the main cost-of-equity regression sample. Panel A reports the full sample of 600 firm-year observations. Panels B and C report the Australian and Chinese subsamples, respectively, with 300 firm-year observations each. CoE denotes the cost of equity used in the main analyses. CSRDS denotes the aggregate cybersecurity-related disclosure score and ranges from 0 to 18. Specificity, Relevance, and Usefulness are the three CSRDS dimension scores, each ranging from 0 to 6. Detailed definitions and measurements of the control variables are provided in Appendix 3D, Table 3D.1.

**Table 4.2***Breakdown of Zero-Score CSRDS Observations*

| Category                                               | Firm-year observations | Percentage                       |
|--------------------------------------------------------|------------------------|----------------------------------|
| CSRDS score = 0                                        | 243                    | 40.5%                            |
| No extracted cybersecurity disclosure                  | 137                    | 56.4% of zero-score observations |
| Cybersecurity related text below the scoring threshold | 106                    | 43.6% of zero-score observations |
| CSRDS score > 0                                        | 357                    | 59.5%                            |

*Note.* This table reports the composition of observations with an aggregate CSRDS score of zero. A zero score may reflect either the absence of extracted cybersecurity related text or the presence of cybersecurity related text that does not meet the minimum threshold for any CSRDS indicator. Percentages for the two zero score categories are calculated relative to the 243 zero score observations.

**4.1.2 Pearson Correlation Matrix**

Table 4.3 reports the Pearson correlation matrix for the CoE regression variables. The table is reported primarily to assess whether the explanatory variables are highly correlated with one another before the multivariate tests are estimated. In line with Table 4.1, the matrix includes the aggregate CSRDS score, the three CSRDS dimensions, and the firm-level controls used in the main analyses.

The bivariate correlations between the cost of equity and aggregate CSRDS, Specificity, Relevance, and Usefulness are positive and statistically significant. These unconditional associations differ from the multivariate regression results reported in Section 4.3, where the corresponding CSRDS coefficients are not statistically significant after controlling for country and firm characteristics and fiscal-year effects. One possible explanation is that the pooled correlations partly reflect differences between the Australian and Chinese samples. Australian firms have higher average CSRDS scores and higher average CAPM-based costs of equity, while the construction of the cost-of-equity measure incorporates country-year risk-free rates and equity risk premia. Differences in these underlying market conditions may therefore contribute to the positive unconditional correlations. The multivariate regressions account for average country differences and observed firm characteristics, resulting in estimates of conditional associations rather than the unconditional relationships captured by the correlations. Accordingly, the positive bivariate correlations should not be interpreted as evidence that more informative CSRDS increases the cost of equity.

The relatively high correlations between the aggregate CSRDS score and the three CSRDS dimensions

are expected because Specificity, Relevance, and Usefulness are components of the aggregate score. These correlations do not create a concern in the main tests because the aggregate score and the dimensions are estimated in separate specifications. The correlations among the three dimensions are lower, indicating that they capture related but distinct aspects of disclosure informativeness. The correlations among the control variables are moderate, with the largest associations observed between ROA and the loss dummy, firm size and liquidity, and firm size and analyst coverage. None of these correlations suggests severe multicollinearity.

Variance inflation factors were also calculated for the final regression specifications and are reported in Appendix 4D, Table 4D.1. The VIF results are generally below 5 in the main models and below the conventional threshold of 10 in the interaction models. On this basis, the correlation matrix and VIF results indicate that multicollinearity is unlikely to affect the main inferences.

**Table 4.3***Pearson Correlation Matrix for the Main CoE Regression Variables*

| <i>Variable</i>         | <i>(1)</i> | <i>(2)</i> | <i>(3)</i> | <i>(4)</i> | <i>(5)</i> | <i>(6)</i> | <i>(7)</i> | <i>(8)</i> | <i>(9)</i> | <i>(10)</i> | <i>(11)</i> | <i>(12)</i> | <i>(13)</i> | <i>(14)</i> |
|-------------------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|-------------|-------------|-------------|-------------|-------------|
| (1) CoE                 | 1.00       |            |            |            |            |            |            |            |            |             |             |             |             |             |
| (2) CSRDS               | 0.11***    | 1.00       |            |            |            |            |            |            |            |             |             |             |             |             |
| (3) Specificity         | 0.09**     | 0.92***    | 1.00       |            |            |            |            |            |            |             |             |             |             |             |
| (4) Relevance           | 0.08**     | 0.81***    | 0.58***    | 1.00       |            |            |            |            |            |             |             |             |             |             |
| (5) Usefulness          | 0.12***    | 0.61***    | 0.42***    | 0.40***    | 1.00       |            |            |            |            |             |             |             |             |             |
| (6) Size                | -0.17***   | 0.22***    | 0.24***    | 0.13***    | 0.12***    | 1.00       |            |            |            |             |             |             |             |             |
| (7) Leverage            | -0.09**    | 0.18***    | 0.22***    | 0.09**     | 0.04       | 0.36***    | 1.00       |            |            |             |             |             |             |             |
| (8) ROA                 | -0.08**    | 0.06       | 0.06       | 0.03       | 0.03       | 0.17***    | -0.11***   | 1.00       |            |             |             |             |             |             |
| (9) Earnings volatility | 0.11***    | -0.04      | -0.04      | -0.01      | -0.05      | -0.27***   | -0.04      | -0.31***   | 1.00       |             |             |             |             |             |
| (10) Analyst coverage   | 0.15***    | 0.38***    | 0.33***    | 0.36***    | 0.21***    | 0.46***    | 0.16***    | 0.18***    | -0.04      | 1.00        |             |             |             |             |
| (11) Loss dummy         | 0.15***    | -0.06      | -0.08*     | -0.03      | -0.02      | -0.29***   | -0.04      | -0.56***   | 0.33***    | -0.19***    | 1.00        |             |             |             |
| (12) Liquidity          | 0.00       | -0.04      | -0.05      | -0.04      | 0.02       | 0.49***    | -0.00      | 0.13***    | -0.09**    | 0.10**      | -0.14***    | 1.00        |             |             |
| (13) Book to market     | -0.01      | 0.13***    | 0.14***    | 0.06       | 0.08**     | 0.28***    | 0.28***    | -0.04      | -0.17***   | 0.05        | 0.04        | -0.17***    | 1.00        |             |
| (14) Listing age        | -0.01      | 0.05       | 0.04       | 0.06       | -0.01      | 0.16***    | 0.33***    | -0.12***   | -0.01      | 0.26***     | 0.03        | -0.06       | 0.08*       | 1.00        |

*Note.* This table reports Pearson correlations for the main regression sample of 600 firm-year observations. CoE denotes the cost of equity used in the main analyses. CSRDS denotes the aggregate cybersecurity-related disclosure score. Specificity, Relevance, and Usefulness are the three CSRDS dimensions. Detailed definitions and measurements of the control variables are provided in Appendix 3D, Table 3D.1. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

## 4.2 H1: Cross-Country Differences in Disclosure Informativeness

Table 4.4 and Figure 4.1 present the country-year pattern in aggregate CSRDS scores. The results show that Australian firm-years have higher CSRDS scores than Chinese firm-years in each fiscal year. In FY2022, the Australian mean CSRDS score is 2.13, compared with 1.21 for China. The gap widens in FY2023, when the Australian mean increases to 3.03 while the Chinese mean remains almost unchanged at 1.28. By FY2024, the Australian mean reaches 3.31, compared with 1.34 for China.

A similar pattern appears in the percentage of firm-years with non-zero CSRDS scores. The proportion of Australian firm-year observations with a positive CSRDS score rises from 66 per cent in FY2022 to 84 per cent in FY2024. The corresponding Chinese proportion remains relatively stable, increasing from 41 per cent to 43 per cent. The widening gap therefore primarily reflects increases in Australian CSRDS scores and the proportion of Australian observations with positive scores, rather than a decline in the corresponding Chinese measures. This descriptive pattern is consistent with H1 and provides context for the formal country comparisons reported below:

**Table 4.4**

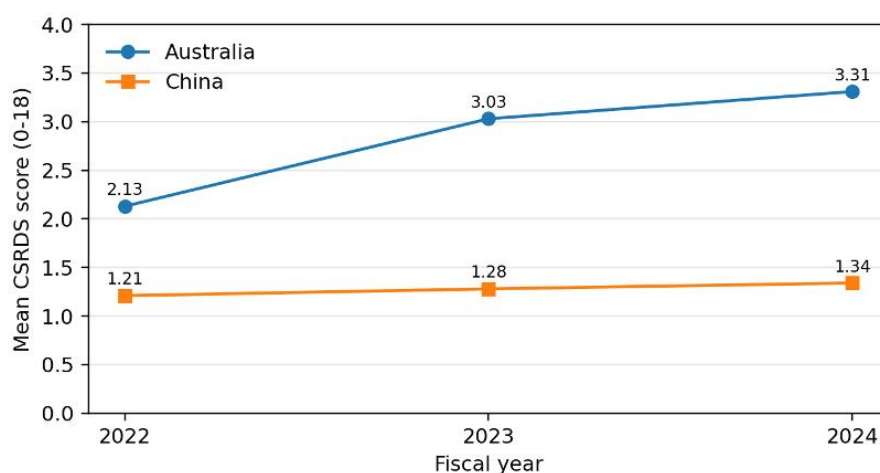
*Mean CSRDS and Positive Score Incidence by Country and Fiscal Year*

| Fiscal year | Australia mean CSRDS score | Australia % with CSRDS score > 0 | China mean CSRDS score | China % with CSRDS score > 0 |
|-------------|----------------------------|----------------------------------|------------------------|------------------------------|
| FY2022      | 2.130                      | 66%                              | 1.210                  | 41%                          |
| FY2023      | 3.030                      | 81%                              | 1.280                  | 42%                          |
| FY2024      | 3.310                      | 84%                              | 1.340                  | 43%                          |

*Note.* This table reports the mean aggregate CSRDS score and the proportion of firm-year observations with a positive CSRDS score in each country and fiscal year. Aggregate CSRDS ranges from 0 to 18. A positive score indicates that at least one CSRDS indicator meets the minimum threshold for a score of 1 or 2. It should not be interpreted as a general disclosure existence measure because some zero score observations contain cybersecurity related text below the scoring threshold. Each country and fiscal year cell contains 100 observations.

**Figure 4.1**

*Mean CSRDS Score by Country, FY2022-FY2024*



*Note.* The figure plots the mean aggregate CSRDS score for Australia and China in each fiscal year. Table 4.5 provides the cross-country aggregate- and dimension-level results for H1.

At the dimension level, the Australian lead extends across all three CSRDS components. Australian firm-years score significantly higher on Specificity, Relevance, and Usefulness. The largest differences appear in Specificity and Relevance, indicating that Australian firms provide more concrete cyber-risk descriptions and more frequently link cybersecurity issues to economically meaningful matters. The difference in Usefulness is smaller, although still statistically significant. Given the low mean Usefulness scores in both countries, quantified or operationally decision-useful cybersecurity disclosure remains uncommon in both markets.

**Table 4.5****Cross-Country Comparison of Aggregate and Dimension-Level CSRDS Scores**

| Variable           | Australia Mean | China Mean | Difference | Welch t | p-value |
|--------------------|----------------|------------|------------|---------|---------|
| CSRDS score (0-18) | 2.823          | 1.277      | +1.55***   | 8.58    | < .001  |
| Specificity (0-6)  | 1.677          | 0.803      | +0.87***   | 7.64    | < .001  |
| Relevance (0-6)    | 0.937          | 0.387      | +0.55***   | 8.09    | < .001  |
| Usefulness (0-6)   | 0.210          | 0.087      | +0.12***   | 3.44    | < .001  |

*Note.* N = 300 Australian and 300 Chinese firm-year observations. Difference = Australia mean minus China mean. Welch t-test is used because it does not assume equal variances across groups. \*, \*\*, and \*\*\* indicate significance at the 10%, 5%, and 1% levels, respectively.

Table 4.6 disaggregates the country difference into the nine CSRDS indicators. The results show that the Australian advantage is broad but uneven. The largest differences appear in S1 and R2. For S1, Australian firm-years are more likely to identify specific cyber threat types than to rely on general references to cyber risk. For R2, Australian firm-years are more likely to connect cyber risk to business consequences, such as operational disruption, value-chain effects, customer impact, or regulatory exposure.

Australian firm-years also score significantly higher on S2, R3, and U2. These results suggest that the Australian lead is concentrated in disclosure attributes that require firms to provide more concrete, consequence-oriented, or exposure-related information. By contrast, S3 and U1 show no significant country difference: few firms in either market disclose cyber risks to key assets or quantified cybersecurity resources, and this disclosure attribute does not distinguish Australian from Chinese reporting practices.

Most indicators show higher values in Australia than in China. The only exception is R1, for which Chinese firm-years record a slightly higher score on active cyber governance in the basic indicator-level comparison. This does not overturn the H1 result, but it suggests that governance or oversight language may be more readily expressed through formal or compliance-oriented reporting. Overall, the indicator-level evidence supports H1 by showing that the Australian advantage is strongest in the more specific and business-consequence-oriented components of cybersecurity disclosure.

**Table 4.6***Cross-Country Comparison of Indicator-Level CSRDS Scores*

| Indicator                                 | Australia Mean | China Mean | Difference | Welch t | p-value |
|-------------------------------------------|----------------|------------|------------|---------|---------|
| S1 Specific cyber threats                 | 0.790          | 0.173      | +0.62***   | 11.18   | < .001  |
| S2 Cyber resilience and readiness         | 0.593          | 0.367      | +0.23***   | 4.24    | < .001  |
| S3 Cyber risks to key assets              | 0.293          | 0.263      | +0.03      | 0.75    | .455    |
| R1 Active cyber governance                | 0.053          | 0.097      | -0.04*     | -1.93   | .054    |
| R2 Cyber risk and business consequences   | 0.500          | 0.080      | +0.42***   | 12.77   | < .001  |
| R3 Third-party and compliance cyber risks | 0.383          | 0.210      | +0.17***   | 4.02    | < .001  |
| U1 Quantified cybersecurity resources     | 0.060          | 0.037      | +0.02      | 1.29    | .199    |
| U2 Cyber insurance and exposure           | 0.063          | 0.003      | +0.06***   | 4.15    | < .001  |
| U3 Cybersecurity performance metrics      | 0.087          | 0.047      | +0.04*     | 1.71    | .088    |

*Note.* Each CSRDS indicator ranges from 0 to 2. The table reports 300 Australian and 300 Chinese firm-year observations. Difference equals the Australian mean minus the Chinese mean. \*, \*\*, and \*\*\* indicate statistical significance at the 10%, 5%, and 1% levels, respectively.

After the aggregate, dimension-level, and indicator-level mean comparisons, Table 4.7 reports the firm-clustered country-difference regressions for H1, i.e., Eq. (3.2). These regressions address the repeated-firm-year structure of the sample by estimating the association between the Australia indicator and each CSRDS measure while controlling for fiscal-year fixed effects and clustering standard errors by firm. The Australia coefficient captures the average difference between Australian and Chinese firm-year observations after accounting for fiscal-year effects.

The indicator-level clustered results are also broadly consistent with the Welch comparisons. The Australia coefficient is positive and significant for S1, S2, R2, R3, and U2, with the largest coefficients again appearing for S1 and R2. These results reinforce the interpretation that the Australian disclosure advantage is concentrated in more concrete and consequence-oriented forms of cybersecurity disclosure. Moreover, there are some weaker indicator-level patterns that become less robust after clustering. Specifically, under the firm-level clustering specification, R1 and U3 are not statistically significant. Therefore, neither R1 nor U3 provides robust support for H1 at the indicator level. The main conclusions of H1 are based on the composite score, the three dimensions, and the

indicators that remain statistically significant after clustering at the firm level.

Overall, the H1 evidence supports the prediction that Australian firms provide more informative cybersecurity related disclosures than Chinese firms. The difference is greatest in S1 and R2, suggesting that the Australian advantage lies mainly in more concrete, business-consequence-oriented disclosure.

**Table 4.7***Firm-Clustered H1 Country-Difference Regression Results*

| Variable                                  | Scale | Australia coef. | Clustered SE | t-statistic | p-value | N   | Adj. R <sup>2</sup> |
|-------------------------------------------|-------|-----------------|--------------|-------------|---------|-----|---------------------|
| CSRDS score                               | 0-18  | 1.547***        | 0.285        | 5.435       | < .001  | 600 | 0.119               |
| Specificity                               | 0-6   | 0.873***        | 0.175        | 4.979       | < .001  | 600 | 0.098               |
| Relevance                                 | 0-6   | 0.550***        | 0.102        | 5.393       | < .001  | 600 | 0.114               |
| Usefulness                                | 0-6   | 0.123**         | 0.053        | 2.307       | .021    | 600 | 0.015               |
| S1 Specific cyber threats                 | 0-2   | 0.617***        | 0.081        | 7.576       | < .001  | 600 | 0.177               |
| S2 Cyber resilience and readiness         | 0-2   | 0.227***        | 0.077        | 2.927       | .003    | 600 | 0.038               |
| S3 Cyber risks to key assets              | 0-2   | 0.030           | 0.058        | 0.514       | .607    | 600 | -0.001              |
| R1 Active cyber governance                | 0-2   | -0.043          | 0.031        | -1.411      | .158    | 600 | 0.004               |
| R2 Cyber risk and business consequences   | 0-2   | 0.420***        | 0.049        | 8.626       | < .001  | 600 | 0.226               |
| R3 Third-party and compliance cyber risks | 0-2   | 0.173***        | 0.062        | 2.781       | .005    | 600 | 0.031               |
| U1 Quantified cybersecurity resources     | 0-2   | 0.023           | 0.026        | 0.895       | .371    | 600 | 0.001               |
| U2 Cyber insurance and exposure           | 0-2   | 0.060***        | 0.021        | 2.818       | .005    | 600 | 0.023               |
| U3 Cybersecurity performance metrics      | 0-2   | 0.040           | 0.033        | 1.211       | .226    | 600 | 0.000               |

*Note.* This table presents the firm-clustered country-difference regressions for H1, i.e., Eq. (3.2). The dependent variable is the CSRDS measure listed in each row. The Australia indicator equals one for Australian firm-year observations and zero for Chinese firm-year observations, so China is the base group. Fiscal-year fixed effects are included but not separately tabulated. Standard errors are clustered by firm. \*, \*\*, and \*\*\* indicate statistical significance at the 10%, 5%, and 1% levels, respectively.

### **4.3 H2: Disclosure Informativeness and the Cost of Equity**

Hypothesis 2 predicts that more informative cybersecurity-related disclosure is associated with a lower cost of equity. The hypothesis is examined in three stages: from the aggregate CSRDS score to its three dimensions, and then to its nine individual indicators. This section reports the main regression results. The robustness analysis in Section 4.5 extends these tests by reestimating the H2 and H3 models using LSEG StarMine WACC as an alternative market based financing cost outcome. This provides a broader financing cost benchmark for comparison with the CAPM based results.

#### **4.3.1 Aggregate and Dimension-level Evidence**

##### **Aggregate evidence**

Table 4.8 reports the aggregate and dimension-level CoE regression results for H2. Column (1) estimates the aggregate CSRDS model specified in Equation (3.3), and column (2) estimates the dimension-level model specified in Equation (3.4). Both models use the cost of equity as the dependent variable and include the Australia indicator, firm-level controls, fiscal-year fixed effects, and firm-clustered standard errors. In column (1), the coefficient on aggregate CSRDS is 0.0003 and is not statistically significant. This result provides no evidence of the negative association predicted by H2. Because the aggregate CSRDS score combines three dimensions and nine indicators, the subsequent analyses examine whether individual disclosure attributes exhibit different associations with the cost of equity.

##### **Dimension evidence**

Table 4.8, column (2), reports the jointly estimated Specificity, Relevance, and Usefulness dimensions. None is statistically significant. Specificity and Usefulness have positive coefficients, while Relevance has the predicted negative sign, but all three coefficients are insignificant. Therefore, the dimension level results do not support H2.

**Table 4.8***H2 Cost of Equity Regressions for Aggregate CSRDS and CSRDS Dimensions*

| Variable                  | (1) Aggregate CSRDS   | (2) CSRDS dimensions  |
|---------------------------|-----------------------|-----------------------|
| CSRDS score               | 0.0003 (0.322)        |                       |
| Specificity               |                       | 0.001<br>(0.645)      |
| Relevance                 |                       | -0.003<br>(-1.347)    |
| Usefulness                |                       | 0.006<br>(1.131)      |
| Australia                 | 0.027***<br>(3.391)   | 0.028***<br>(3.482)   |
| Firm size                 | -0.006***<br>(-3.636) | -0.006***<br>(-3.742) |
| Leverage                  | -0.007<br>(-1.333)    | -0.007<br>(-1.349)    |
| ROA                       | -0.008<br>(-0.785)    | -0.008<br>(-0.809)    |
| Earnings volatility       | 0.000<br>(0.015)      | 0.001<br>(0.037)      |
| Analyst coverage          | 0.002<br>(0.883)      | 0.002<br>(0.982)      |
| Loss dummy                | 0.003<br>(0.784)      | 0.003<br>(0.740)      |
| Liquidity                 | 0.007***<br>(3.209)   | 0.008***<br>(3.317)   |
| Book-to-market            | 0.008<br>(1.346)      | 0.008<br>(1.392)      |
| Listing age               | -0.004*<br>(-1.858)   | -0.004*<br>(-1.880)   |
| Fiscal year fixed effects | Yes                   | Yes                   |
| Firm-clustered SE         | Yes                   | Yes                   |
| N                         | 600                   | 600                   |
| Adjusted R <sup>2</sup>   | 0.245                 | 0.252                 |

*Note.* The dependent variable is the CAPM-based cost of equity. Column (1) reports the aggregate CSRDS model specified in Equation (3.3), which provides the primary test of H2. Column (2) reports the dimension model specified in Equation (3.4), in which Specificity, Relevance, and Usefulness are entered jointly. Both models include the Australia indicator, the firm level controls defined in Appendix 3D, Table 3D.1, and fiscal year fixed effects. Fiscal year coefficients are included but not separately reported. The t statistics in parentheses are based on standard errors clustered by firm. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

### 4.3.2 Indicator-Level Results

The analysis next disaggregates CSRDS into its nine indicators. According to Table 4.9, Equation (3.5) enters all nine CSRDS indicators simultaneously. Therefore, each coefficient captures the association between the relevant indicator and the cost of equity after controlling for the other eight indicators, the Australia indicator, the firm-level controls, and fiscal year fixed effects. This analysis supplements the aggregate test of H2 by examining whether particular disclosure attributes have distinct associations with the cost of equity.

As Table 4.9 reports, eight of the nine CSRDS indicator coefficients are not statistically significant. Only R2 shows a negative and statistically significant association with the cost of equity, with a coefficient of  $-0.0156$  and a  $t$  statistic of  $-3.59$ . By comparison, U2 has a positive coefficient of  $0.0127$ , which is similar in absolute magnitude but is not statistically significant ( $t = 1.00$ ). This comparison illustrates that a statistically insignificant coefficient is not necessarily small in magnitude; its statistical significance also depends on estimation precision. As defined in Section 3.3.2, R2 captures whether firms link cyber risk to operational or financial consequences through specific business processes. The negative R2 coefficient therefore indicates a conditional association between more informative business-consequence disclosure and a lower cost of equity, after controlling for the other eight indicators and the remaining model variables.

Figure 4.2 presents the coefficients and 95 per cent confidence intervals from the joint indicator model. As shown in the figure, the confidence interval for R2 is the only interval that lies entirely below zero, while the intervals for the other eight indicators cross zero. Therefore, the figure provides a visual representation of the results in Table 4.9 and illustrates that R2 is the only indicator whose coefficient is statistically distinguishable from zero in the joint specification.

Supplementary single indicator specifications for the nine CSRDS indicators are reported in Appendix 4A. Table 4A.2. When each indicator is entered separately using the same control structure, the coefficient on R2 remains negative and statistically significant. The R2 coefficient is negative in both the joint and separate-indicator specifications. However, because multiple related indicator tests are examined, the unadjusted significance of these estimates should not by itself be interpreted as evidence of robustness. Multiplicity-adjusted inference is reported in Section 4.5.

Collectively, the indicator-level results suggest that the association between cybersecurity-related disclosure and the cost of equity is not uniform across disclosure attributes, and composite measures do not exhibit a uniform association across their underlying components. However, the indicator-level evidence does not establish that R2 explains the aggregate or dimension-level results. H2 therefore remains unsupported at the aggregate CSRDS level. The R2 finding is interpreted as supplementary evidence that disclosure linking cyber risk to operational or financial business consequences is associated with the cost of equity, rather than as evidence of a general association for overall CSRDS informativeness.

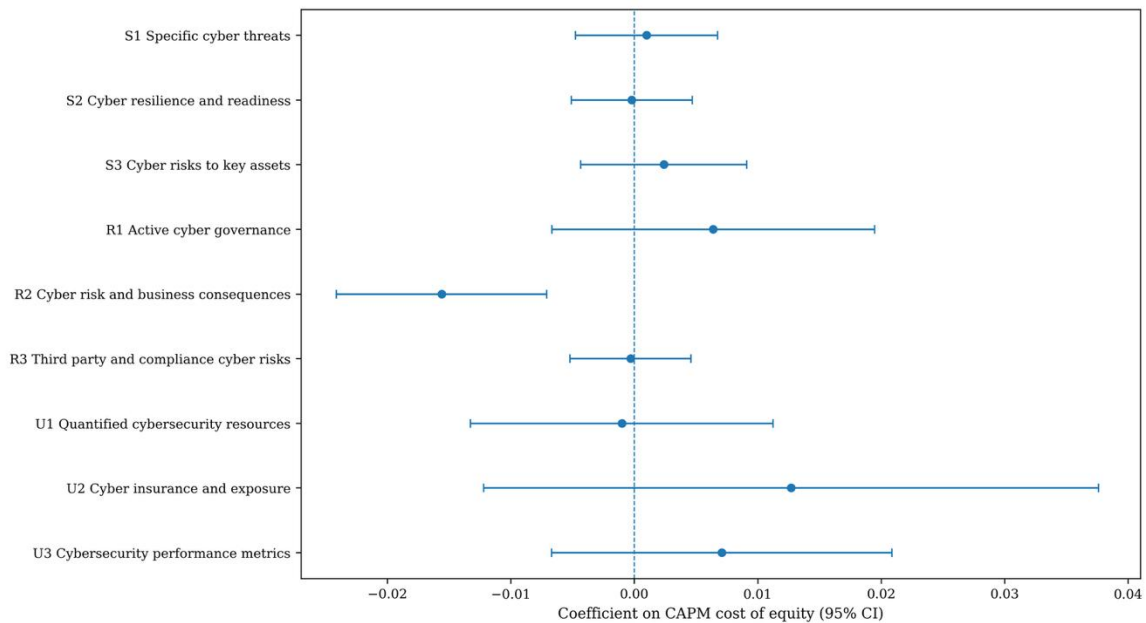
**Table 4.9***Joint Indicator Model of CSRDS and Cost of Equity*

| Variable                                  | (1) Joint indicator model |
|-------------------------------------------|---------------------------|
| S1 Specific cyber threats                 | 0.0010<br>(0.34)          |
| S2 Cyber resilience and readiness         | -0.0002<br>(-0.08)        |
| S3 Cyber risks to key assets              | 0.0024<br>(0.70)          |
| R1 Active cyber governance                | 0.0064<br>(0.96)          |
| R2 Cyber risk and business consequences   | -0.0156***<br>(-3.59)     |
| R3 Third-party and compliance cyber risks | -0.0003<br>(-0.12)        |
| U1 Quantified cybersecurity resources     | -0.0010<br>(-0.16)        |
| U2 Cyber insurance and exposure           | 0.0127<br>(1.00)          |
| U3 Cybersecurity performance metrics      | 0.0071<br>(1.01)          |
| Australia                                 | 0.0354***<br>(4.78)       |
| Firm size                                 | -0.0061***<br>(-3.74)     |
| Leverage                                  | -0.0048<br>(-0.87)        |
| ROA                                       | -0.0072<br>(-0.76)        |
| Earnings volatility                       | -0.0039<br>(-0.17)        |
| Analyst coverage                          | 0.0018<br>(0.81)          |
| Loss dummy                                | 0.0006<br>(0.15)          |
| Liquidity                                 | 0.0085***<br>(4.00)       |
| Book to market                            | 0.0089*<br>(1.71)         |
| Listing age                               | -0.0039*<br>(-1.85)       |
| Fiscal year fixed effects                 | Yes                       |
| Firm clustered standard errors            | Yes                       |
| Observations                              | 600                       |
| Adjusted R <sup>2</sup>                   | 0.277                     |

*Note.* This table presents the joint indicator model specified in Equation (3.5). The dependent variable is cost of equity. All nine CSRDS indicators are entered simultaneously. Coefficients are reported with firm clustered t statistics in parentheses. Standard errors are clustered by firm. The model includes the Australia indicator, firm level controls, and fiscal year fixed effects. FY2022 is the omitted fiscal year. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

**Figure 4.2**

*Indicator-Level Coefficients on the Cost of Equity*



*Note.* The figure plots the coefficients for each of the nine indicators from the joint indicator model for the main cost-of-equity measure, reported in Table 4.9, with horizontal bars showing the 95 per cent confidence intervals.

### 4.3.3 Summary of H2 Evidence

Overall, the aggregate- and dimension-level results do not support H2. Neither the aggregate CSRDS measure nor any of the three dimension scores is significantly associated with the cost of equity. Accordingly, these results do not provide evidence of a general negative association between broad CSRDS informativeness and the cost of equity.

However, at the indicator level, a more specific pattern emerges. In the joint indicator model reported in Table 4.9, R2 is the only indicator with a negative and statistically significant coefficient (coefficient = -0.0156,  $t = -3.59$ ). R2 captures whether a firm links cyber risk to operational or financial consequences through specific business processes. Holding the other eight indicators and the remaining model variables constant, a one-point increase in R2 is associated with a 1.56 percentage point lower cost of equity. Relative to the sample mean cost of equity of 9.4 per cent and its standard deviation of 3.1 percentage points, this estimate represents an economically sizeable association. Because the analysis is observational and R2 is measured on an ordinal scale, the magnitude should be interpreted as a conditional association rather than a causal effect.

These supplementary results do not alter the formal conclusion for H2. H2 remains unsupported at the aggregate CSRDS level. Taken together, the evidence suggests that the association with a lower cost of equity is not evident for CSRDS as a broad composite measure, but is concentrated in disclosures that link cyber risk to concrete business consequences.

#### **4.4 H3: Country Moderation of the Association between CSRDS and the Cost of Equity**

H3 predicts that the negative association between cybersecurity disclosure informativeness and the cost of equity is stronger in Australia than in China. The aggregate interaction model specified in Equation (3.6) provides the primary test of H3. This model interacts aggregate CSRDS with the Australia indicator, so the interaction coefficient measures the difference between the Australian and Chinese slopes. Equation (3.7) provides a supplementary interaction analysis for R2, Cyber risk and business consequences, because R2 is the only indicator with a negative and statistically significant coefficient in the joint indicator model. Country specific regressions are reported in Appendix 4B, Table 4B.1 as supplementary evidence.

Table 4.10 reports the CoE interaction regressions for H3. In column (1), the coefficient on  $\text{CSRDS score} \times \text{Australia}$  is negative but not statistically significant. This indicates that the association between aggregate CSRDS and the cost of equity is not statistically stronger for Australian firms than for Chinese firms. Therefore, the formal aggregate interaction test does not support H3. Column (2) reports the supplementary R2 interaction model. The coefficient on  $\text{R2} \times \text{Australia}$  is also not statistically significant. This indicates that although R2 is the strongest pricing-related disclosure attribute in the H2 analysis, the R2 pricing association does not differ significantly between Australia and China in the formal interaction test.

The country specific regressions reported in Appendix 4B, Table 4B.1 show that R2 is negative and statistically significant in the Australian subsample but not in the Chinese subsample, suggesting that the full sample R2 association is more evident in Australia. However, the  $\text{R2} \times \text{Australia}$  interaction is not statistically significant, so this subsample pattern does not establish that the two country coefficients differ significantly. Accordingly, neither the aggregate CSRDS interaction nor the supplementary R2 interaction supports H3.

**Table 4.10**  
*H3 CoE Interaction Regression Results*

| Variable                | (1) CSRDS score interaction | (2) R2 indicator interaction |
|-------------------------|-----------------------------|------------------------------|
| CSRDS score             | 0.0009<br>(0.82)            |                              |
| R2 indicator            |                             | -0.0127<br>(-1.19)           |
| Australia               | 0.0297***<br>(3.76)         | 0.0343***<br>(4.52)          |
| CSRDS score × Australia | -0.0011<br>(-0.55)          |                              |
| R2 × Australia          |                             | 0.0008<br>(0.07)             |
| Firm size               | -0.0058***<br>(-3.75)       | -0.0059***<br>(-3.83)        |
| Leverage                | -0.0069<br>(-1.32)          | -0.0049<br>(-0.88)           |
| ROA                     | -0.0075<br>(-0.78)          | -0.0075<br>(-0.77)           |
| Earnings volatility     | -0.0009<br>(-0.04)          | -0.0032<br>(-0.13)           |
| Analyst coverage        | 0.0020<br>(0.86)            | 0.0024<br>(1.13)             |
| Loss dummy              | 0.0032<br>(0.76)            | 0.0017<br>(0.42)             |
| Liquidity               | 0.0076***<br>(3.49)         | 0.0083***<br>(3.73)          |
| Book-to-market          | 0.0082<br>(1.31)            | 0.0095<br>(1.57)             |
| Listing age             | -0.0039*<br>(-1.78)         | -0.0046**<br>(-2.03)         |
| FY2023                  | 0.0190***<br>(11.18)        | 0.0201***<br>(12.61)         |
| FY2024                  | 0.0033**<br>(2.54)          | 0.0050***<br>(4.05)          |
| Year fixed effects      | Yes                         | Yes                          |
| Firm-clustered SE       | Yes                         | Yes                          |
| N                       | 600                         | 600                          |
| Adjusted R <sup>2</sup> | 0.245                       | 0.265                        |

*Note.* The dependent variable is cost of equity. China is the reference group, and the interaction terms capture the incremental Australian slope. Firm-clustered t-statistics are reported in parentheses, and FY2022 is the omitted year. \*, \*\*, and \*\*\* denote statistical significance at the 10%, 5%, and 1% levels, respectively.

## 4.5 Robustness and Sensitivity Analyses

Table 4.11 reports selected coefficients from four sets of robustness checks, while the full results are reported in Appendix 4C, Tables 4C.1 to 4C.4. These analyses build on the H2 and H3 models and examine the stability of the main findings across an alternative market based financing cost outcome, winsorised variables, alternative treatments of zero and positive CSRDS observations, and additional governance controls. Particular attention is given to whether the R2 result remains observable across these specifications.

**Alternative market based financing cost outcome.** Panel A reestimates the H2 and H3 models using LSEG StarMine WACC, obtained through LSEG Workspace, as the dependent variable. WACC incorporates the weighted costs of debt, common equity, and preferred equity and therefore provides a broader financing cost outcome than the CAPM based cost of equity used in the main analysis. One missing LSEG WACC observation was replaced with the corresponding CAPM based cost of equity value. Because WACC and CAPM based cost of equity are related but not equivalent financing cost measures, this substitution is an approximation.<sup>1</sup> The results are broadly consistent with the main findings. The aggregate CSRDS score remains statistically insignificant, while R2 remains negative under the LSEG WACC specification and is statistically significant using unadjusted inference. However, the R2 association is no longer statistically significant after the Holm multiple-testing adjustment, as reported in Table 4.14. The  $R2 \times \text{Australia}$  interaction remains statistically insignificant, indicating that the R2 association does not differ significantly between Australia and China under the LSEG WACC specification. The Relevance dimension is also negative and statistically significant at the 10 per cent level in the LSEG WACC specification, although it is not statistically significant in the main CAPM model.

**Winsorised estimates.** Panel B compares the focal coefficients from the original CAPM models with those obtained after the relevant continuous variables are winsorised at the 1st and 99th percentiles. Aggregate CSRDS and the three dimension coefficients remain statistically insignificant. The R2 only coefficient remains negative and statistically significant, while the aggregate CSRDS interaction

---

<sup>1</sup> The statistical inferences remain unchanged when the missing LSEG WACC observation is not replaced and the full sample models are estimated using 599 observations.

remains statistically insignificant. The persistence of the R2 coefficient after winsorisation reduces concern that the reported association is driven primarily by extreme observations.

**Zero and positive CSRDS observations.** Panel C first replaces aggregate CSRDS with a positive CSRDS indicator that equals one when at least one CSRDS indicator receives a positive score and zero otherwise. The coefficient on this indicator is not statistically significant under either reported specification. This result provides no evidence that crossing the minimum threshold for a positive CSRDS score is associated with financing costs in either the CAPM or LSEG WACC specification.

Panel C also estimates the aggregate CSRDS and R2 models using the subsample of firm-year observations with positive CSRDS scores. Aggregate CSRDS remains statistically insignificant in both positive CSRDS subsamples. R2 remains negative and statistically significant in the CAPM specification, while the corresponding R2 coefficient in the LSEG WACC specification is negative but not statistically significant. These results indicate that the R2 association remains observable in the CAPM model after zero score observations are excluded, although the corresponding evidence is weaker under the LSEG WACC specification.

**Governance controls.** Panel D adds board independence and board size in the governance subsample. The aggregate CSRDS score remains statistically insignificant after governance controls are added in the CAPM specification. R2 remains negative and statistically significant in the CAPM governance-control specification. In the corresponding LSEG WACC specification, the R2 coefficient remains negative but is not statistically significant. These results suggest that the CAPM R2 association is not simply explained by observable board governance characteristics, although the corresponding evidence is weaker under the alternative financing cost outcome. Because this test is based on a smaller subsample and includes only selected board variables, it should be interpreted as supplementary robustness evidence rather than causal evidence.

**Table 4.11***Selected Robustness and Sensitivity Results*

| <b>Panel A. Alternative Market Based Financing Cost Outcome Using LSEG WACC</b> |                      |                       |                      |                              |                           |
|---------------------------------------------------------------------------------|----------------------|-----------------------|----------------------|------------------------------|---------------------------|
| <b>Variable</b>                                                                 | <b>(1) Aggregate</b> | <b>(2) Dimensions</b> | <b>(3) R2</b>        | <b>(4) CSRDS × Australia</b> | <b>(5) R2 × Australia</b> |
| CSRDS score                                                                     | −0.0005<br>(−0.71)   |                       |                      | −0.0012<br>(−1.52)           |                           |
| Specificity                                                                     |                      | 0.0012<br>(0.94)      |                      |                              |                           |
| Relevance                                                                       |                      | −0.0039*<br>(−1.83)   |                      |                              |                           |
| Usefulness                                                                      |                      | −0.0003<br>(−0.07)    |                      |                              |                           |
| R2 Cyber risk and business consequences                                         |                      |                       | −0.0079**<br>(−2.18) |                              | −0.0146**<br>(−2.30)      |
| Australia                                                                       | 0.0090<br>(1.20)     | 0.0094<br>(1.27)      | 0.0126*<br>(1.67)    | 0.0057<br>(0.76)             | 0.0105<br>(1.38)          |
| CSRDS score × Australia                                                         |                      |                       |                      | 0.0013<br>(0.95)             |                           |
| R2 × Australia                                                                  |                      |                       |                      |                              | 0.0088<br>(1.11)          |
| Observations                                                                    | 600                  | 600                   | 600                  | 600                          | 600                       |
| Adjusted R <sup>2</sup>                                                         | 0.132                | 0.138                 | 0.143                | 0.133                        | 0.145                     |
| <b>Panel B. Original and Winsorised CAPM estimates</b>                          |                      |                       |                      |                              |                           |
| <b>Variable</b>                                                                 | <b>(1) Original</b>  | <b>(2) Winsorised</b> |                      |                              |                           |
| CSRDS score                                                                     |                      | 0.0003<br>(0.32)      |                      | −0.0001<br>(−0.09)           |                           |
| Specificity                                                                     |                      | 0.0009<br>(0.65)      |                      | 0.0006<br>(0.45)             |                           |
| Relevance                                                                       |                      | −0.0032<br>(−1.35)    |                      | −0.0026<br>(−1.14)           |                           |
| Usefulness                                                                      |                      | 0.0058<br>(1.13)      |                      | 0.0028<br>(0.85)             |                           |
| R2 Cyber risk and business consequences                                         |                      | −0.0121***<br>(−2.83) |                      | −0.0124***<br>(−3.12)        |                           |
| CSRDS score × Australia                                                         |                      | −0.0011<br>(−0.55)    |                      | −0.0019<br>(−1.24)           |                           |
| Observations                                                                    |                      | 600                   |                      | 600                          |                           |

**Panel C. Positive CSRDS Indicator and Positive CSRDS Subsample Analyses**

| Variable                                | (1) CAPM full sample | (2) CAPM positive CSRDS subsample: CSRDS | (3) CAPM positive CSRDS subsample: R2 | (4) LSEG full sample | (5) LSEG positive CSRDS subsample: CSRDS | (6) LSEG positive CSRDS subsample: R2 |
|-----------------------------------------|----------------------|------------------------------------------|---------------------------------------|----------------------|------------------------------------------|---------------------------------------|
| Positive CSRDS indicator                | -0.0038<br>(-1.25)   |                                          |                                       | -0.0039<br>(-1.32)   |                                          |                                       |
| CSRDS score                             |                      | 0.0019<br>(1.60)                         |                                       |                      | 0.0004<br>(0.48)                         |                                       |
| R2 Cyber risk and business consequences |                      |                                          | -0.0097**<br>(-2.33)                  |                      |                                          | -0.0065<br>(-1.58)                    |
| Observations                            | 600                  | 357                                      | 357                                   | 600                  | 357                                      | 357                                   |
| Adjusted R <sup>2</sup>                 | 0.248                | 0.228                                    | 0.231                                 | 0.135                | 0.218                                    | 0.227                                 |

**Panel D. CAPM Governance Control Sensitivity Analyses**

| Variable                                | (1) CSRDS baseline | (2) CSRDS with governance | (3) R2 baseline       | (4) R2 with governance | (5) Relevance baseline | (6) Relevance with governance |
|-----------------------------------------|--------------------|---------------------------|-----------------------|------------------------|------------------------|-------------------------------|
| CSRDS score                             | -0.0004<br>(-0.26) | 0.0003<br>(0.16)          |                       |                        |                        |                               |
| R2 Cyber risk and business consequences |                    |                           | -0.0173***<br>(-3.55) | -0.0157***<br>(-3.13)  |                        |                               |
| Relevance dimension                     |                    |                           |                       |                        | -0.0055*<br>(-1.74)    | -0.0048<br>(-1.50)            |
| Governance controls                     | No                 | Yes                       | No                    | Yes                    | No                     | Yes                           |
| Observations                            | 293                | 293                       | 293                   | 293                    | 293                    | 293                           |
| Firms                                   | 102                | 102                       | 102                   | 102                    | 102                    | 102                           |
| Adjusted R <sup>2</sup>                 | 0.249              | 0.271                     | 0.295                 | 0.308                  | 0.265                  | 0.286                         |

*Note.* This table reports selected coefficients from the robustness and sensitivity analyses. Panel A reports the LSEG WACC specifications. Panel B compares focal coefficients from the corresponding original and winsorised CAPM models. Each row in Panel B represents a separate regression specification. Panel C reports the positive CSRDS indicator and positive CSRDS subsample analyses. A positive CSRDS score indicates that at least one CSRDS indicator meets the minimum scoring threshold and should not be interpreted as a general measure of disclosure existence. Panel D compares baseline and governance augmented CAPM models using the same subsample of 293 firm-year observations from 102 firms. The t statistics are reported in parentheses. Blank cells indicate that the relevant variable is not included in the specification. Full results are reported in Appendix 4C, Tables 4C.1 to 4C.4. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

**H1 broad sector fixed effects robustness test.** Table 4.12 reports an additional robustness test for H1 in which the aggregate CSRDS country difference model is reestimated with broad sector fixed effects. The Australia coefficient remains positive and statistically significant after the sector fixed effects are included. Specifically, the coefficient decreases only moderately from 1.547 in the baseline model to 1.461 in the sector adjusted model and remains significant at the 1 per cent level. This result indicates that the aggregate difference in CSRDS informativeness between Australian and Chinese firms is not attributable solely to systematic differences across the three sampled sectors.

Overall, the H1 result remains robust to broad sector fixed effects. Turning to H2 and H3, the aggregate CSRDS coefficient remains insignificant, while R2 retains a negative coefficient in the main CAPM model and several robustness specifications. The H3 interaction terms are insignificant, offering no support for H3. In the CAPM joint-indicator analysis, R2 is the strongest supplementary indicator-level finding, holding statistical significance after both industry adjustment and the Holm multiple-testing correction. This evidence is weaker in the separate-indicator and LSEG specifications.

**Table 4.12**

*Additional H1 Robustness Test with Broad Sector Fixed Effects*

| Variable                       | (1) Baseline H1 model | (2) Broad sector fixed effects model |
|--------------------------------|-----------------------|--------------------------------------|
| Australia                      | 1.547***<br>(5.435)   | 1.461***<br>(4.707)                  |
| Fiscal year fixed effects      | Yes                   | Yes                                  |
| Broad sector fixed effects     | No                    | Yes                                  |
| Firm clustered standard errors | Yes                   | Yes                                  |
| Observations                   | 600                   | 600                                  |
| Adjusted R <sup>2</sup>        | 0.119                 | 0.135                                |

*Note.* The dependent variable is the aggregate CSRDS score. Column (1) reproduces the baseline H1 specification reported in Table 4.7. Column (2) additionally includes broad sector fixed effects for Healthcare and Technology, with Financials serving as the reference sector. The Australia indicator equals one for Australian firm year observations and zero for Chinese firm year observations. Firm clustered t statistics are reported in parentheses. \*\*\*, \*\*, and \* indicate statistical significance at the 1 per cent, 5 per cent, and 10 per cent levels, respectively.

Table 4.13 re-estimates the principal H2 and H3 specifications with broad industry fixed effects for Healthcare and Technology, using Financials as the reference category. This comparison assesses whether the materially different industry composition of the Australian and Chinese samples affects the principal cost-of-equity conclusions.

For the primary CAPM H2 specification, the aggregate CSRDS coefficient is 0.000302 without industry fixed effects and 0.000300 with them included. Both estimates remain statistically insignificant. Industry adjustment therefore leaves the aggregate H2 conclusion unchanged, and the three jointly estimated dimension coefficients also remain statistically insignificant.

The aggregate H3 interaction conclusion is likewise unchanged. The  $\text{CSRDS} \times \text{Australia}$  coefficient moves from -0.001078 without industry fixed effects to -0.000860 with them, and remains statistically insignificant in both specifications ( $p = .584$  and  $p = .665$ , respectively). The industry-adjusted analysis thus continues to provide no support for H3.

The Australia coefficient remains positive and statistically significant in the CAPM aggregate H2 specifications, but not in the corresponding LSEG WACC specifications. This difference should be interpreted in light of the distinct financing-cost measures rather than as evidence of a causal country effect.

**Table 4.13***Industry fixed-effects robustness results***Panel A. CAPM-based cost-of-equity results**

| Variable                   | (1) Aggregate<br>No FE | (2) Aggregate<br>Industry FE | (3) Dimensions<br>No FE | (4) Dimensions<br>Industry FE | (5) Interaction<br>No FE | (6) Interaction<br>Industry FE |
|----------------------------|------------------------|------------------------------|-------------------------|-------------------------------|--------------------------|--------------------------------|
| CSRDS score                | 0.0003<br>(0.32)       | 0.0003<br>(0.32)             |                         |                               | 0.0009<br>(0.82)         | 0.0008<br>(0.69)               |
| Specificity                |                        |                              | 0.0009<br>(0.65)        | 0.0009<br>(0.62)              |                          |                                |
| Relevance                  |                        |                              | -0.0032<br>(-1.35)      | -0.0027<br>(-1.17)            |                          |                                |
| Usefulness                 |                        |                              | 0.0058<br>(1.13)        | 0.0049<br>(0.97)              |                          |                                |
| Australia                  | 0.0270***<br>(3.39)    | 0.0245***<br>(3.14)          | 0.0277***<br>(3.48)     | 0.0257***<br>(3.23)           | 0.0297***<br>(3.76)      | 0.0267***<br>(3.40)            |
| CSRDS score ×<br>Australia |                        |                              |                         |                               | -0.0011<br>(-0.55)       | -0.0009<br>(-0.43)             |
| Firm-level controls        | Yes                    | Yes                          | Yes                     | Yes                           | Yes                      | Yes                            |
| Year fixed effects         | Yes                    | Yes                          | Yes                     | Yes                           | Yes                      | Yes                            |
| Industry fixed effects     | No                     | Yes                          | No                      | Yes                           | No                       | Yes                            |
| Observations               | 600                    | 600                          | 600                     | 600                           | 600                      | 600                            |
| Firms                      | 200                    | 200                          | 200                     | 200                           | 200                      | 200                            |
| Adjusted R <sup>2</sup>    | 0.245                  | 0.252                        | 0.252                   | 0.256                         | 0.245                    | 0.251                          |

**Panel B. LSEG WACC results**

| Variable    | (1) Aggregate<br>No FE | (2) Aggregate<br>Industry FE | (3) Dimensions<br>No FE | (4) Dimensions<br>Industry FE | (5) Interaction<br>No FE | (6) Interaction<br>Industry FE |
|-------------|------------------------|------------------------------|-------------------------|-------------------------------|--------------------------|--------------------------------|
| CSRDS score | -0.0005<br>(-0.71)     | -0.0005<br>(-0.73)           |                         |                               | -0.0012<br>(-1.52)       | -0.0013<br>(-1.60)             |
| Specificity |                        |                              | 0.0012<br>(0.94)        | 0.0012<br>(0.94)              |                          |                                |
| Relevance   |                        |                              | -0.0039*<br>(-1.83)     | -0.0038*<br>(-1.92)           |                          |                                |
| Usefulness  |                        |                              | -0.0003<br>(-0.07)      | -0.0006<br>(-0.15)            |                          |                                |
| Australia   | 0.0090<br>(1.20)       | 0.0080<br>(1.07)             | 0.0094<br>(1.27)        | 0.0088<br>(1.18)              | 0.0057<br>(0.76)         | 0.0043<br>(0.59)               |

|                         |       |       |       |       |        |        |
|-------------------------|-------|-------|-------|-------|--------|--------|
| CSRDS score ×           |       |       |       |       | 0.0013 | 0.0014 |
| Australia               |       |       |       |       | (0.95) | (1.04) |
| Firm-level controls     | Yes   | Yes   | Yes   | Yes   | Yes    | Yes    |
| Year fixed effects      | Yes   | Yes   | Yes   | Yes   | Yes    | Yes    |
| Industry fixed effects  | No    | Yes   | No    | Yes   | No     | Yes    |
| Observations            | 600   | 600   | 600   | 600   | 600    | 600    |
| Firms                   | 200   | 200   | 200   | 200   | 200    | 200    |
| Adjusted R <sup>2</sup> | 0.132 | 0.131 | 0.138 | 0.137 | 0.133  | 0.133  |

*Note.* This table reports the H2 and H3 robustness results with and without broad industry fixed effects. Coefficients are reported with firm-clustered t-statistics in parentheses. Statistical inference uses a two-sided Student's t-distribution with 199 degrees of freedom (200 firm clusters minus one). \*, \*\*, and \*\*\* indicate statistical significance at the 10%, 5%, and 1% levels, respectively. Blank cells indicate that the relevant variable is not included in the specification. All models include the nine firm-level controls and fiscal-year fixed effects.

Table 4.14 reports the joint nine-indicator models with and without industry fixed effects, along with unadjusted and Holm-adjusted p values for the 18-test indicator family defined in Section 3.6.

In the CAPM joint model,  $R^2$  is negative and remains statistically significant after multiplicity adjustment. Without industry fixed effects, the  $R^2$  coefficient is  $-0.015579$  (unadjusted  $p = .000420$ ; Holm-adjusted  $p = .007552$ ). With industry fixed effects, the coefficient is  $-0.015978$  (unadjusted  $p = .000317$ ; Holm-adjusted  $p = .005713$ ). Industry adjustment therefore leaves the magnitude and inference materially unchanged, and  $R^2$  remains significant in the CAPM joint specification after multiple-testing adjustment.

The LSEG joint results are weaker.  $R^2$  is negative and statistically significant under unadjusted inference both without and with industry fixed effects, but the Holm-adjusted p values are .273747 and .260242, respectively. The LSEG  $R^2$  result therefore does not survive the same multiple-testing adjustment.

The supplementary separate-indicator CAPM  $R^2$  coefficient is also negative, but its Holm-adjusted inference under the same 18-test family does not reach the 5 per cent threshold. The multiplicity-adjusted evidence is thus strongest for the CAPM joint specification, rather than uniform across all indicator specifications.

**Table 4.14***Holm-adjusted results for the indicator-level analyses***Panel A. CAPM joint-indicator models**

| Variable                | (1) No industry FE    | (2) Industry FE       | (3) Holm p<br>No industry FE | (4) Holm p<br>Industry FE |
|-------------------------|-----------------------|-----------------------|------------------------------|---------------------------|
| S1                      | 0.0010<br>(0.34)      | 0.0014<br>(0.50)      | 1.000000                     | 1.000000                  |
| S2                      | -0.0002<br>(-0.08)    | -0.0004<br>(-0.17)    | 1.000000                     | 1.000000                  |
| S3                      | 0.0024<br>(0.70)      | 0.0020<br>(0.61)      | 1.000000                     | 1.000000                  |
| R1                      | 0.0064<br>(0.96)      | 0.0065<br>(0.99)      | 1.000000                     | 1.000000                  |
| R2                      | -0.0156***<br>(-3.59) | -0.0160***<br>(-3.66) | 0.007552                     | 0.005713                  |
| R3                      | -0.0003<br>(-0.12)    | 0.0013<br>(0.46)      | 1.000000                     | 1.000000                  |
| U1                      | -0.0010<br>(-0.16)    | -0.0046<br>(-0.71)    | 1.000000                     | 1.000000                  |
| U2                      | 0.0127<br>(1.00)      | 0.0121<br>(0.96)      | 1.000000                     | 1.000000                  |
| U3                      | 0.0071<br>(1.01)      | 0.0070<br>(1.00)      | 1.000000                     | 1.000000                  |
| Observations            | 600                   | 600                   |                              |                           |
| Firms                   | 200                   | 200                   |                              |                           |
| Adjusted R <sup>2</sup> | 0.277                 | 0.287                 |                              |                           |

**Panel B. LSEG WACC joint-indicator models**

| Variable | (1) No industry FE   | (2) Industry FE      | (3) Holm p<br>No industry FE | (4) Holm p<br>Industry FE |
|----------|----------------------|----------------------|------------------------------|---------------------------|
| S1       | 0.0018<br>(0.75)     | 0.0019<br>(0.78)     | 1.000000                     | 1.000000                  |
| S2       | 0.0011<br>(0.43)     | 0.0010<br>(0.42)     | 1.000000                     | 1.000000                  |
| S3       | 0.0016<br>(0.53)     | 0.0015<br>(0.50)     | 1.000000                     | 1.000000                  |
| R1       | -0.0052<br>(-1.19)   | -0.0052<br>(-1.22)   | 1.000000                     | 1.000000                  |
| R2       | -0.0092**<br>(-2.45) | -0.0094**<br>(-2.47) | 0.273747                     | 0.260242                  |

|                         |                    |                    |          |          |
|-------------------------|--------------------|--------------------|----------|----------|
| R3                      | -0.0007<br>(-0.22) | -0.0002<br>(-0.07) | 1.000000 | 1.000000 |
| U1                      | -0.0030<br>(-0.76) | -0.0043<br>(-0.92) | 1.000000 | 1.000000 |
| U2                      | 0.0142<br>(1.47)   | 0.0140<br>(1.48)   | 1.000000 | 1.000000 |
| U3                      | -0.0045<br>(-0.76) | -0.0047<br>(-0.79) | 1.000000 | 1.000000 |
| Observations            | 600                | 600                |          |          |
| Firms                   | 200                | 200                |          |          |
| Adjusted R <sup>2</sup> | 0.147              | 0.147              |          |          |

**Panel C. Separate R2 results and Holm-adjusted p values**

| <b>Outcome</b> | <b>(1) No industry FE</b> | <b>(2) Industry FE</b> | <b>(3) Holm p<br/>No industry FE</b> | <b>(4) Holm p<br/>Industry FE</b> |
|----------------|---------------------------|------------------------|--------------------------------------|-----------------------------------|
| CAPM           | -0.0121***<br>(-2.83)     | -0.0125***<br>(-2.97)  | 0.086572                             | 0.056464                          |
| LSEG WACC      | -0.0079**<br>(-2.18)      | -0.0081**<br>(-2.22)   | 0.522842                             | 0.464080                          |

*Note.* This table reports the joint nine-indicator models and supplementary separate R2 results, together with Holm-adjusted p-values. Columns (1) and (2) report coefficients with firm-clustered t statistics in parentheses. Columns (3) and (4) report Holm-adjusted p values for the predefined 18-test family within each outcome and industry fixed-effects setting. Inference uses a two-sided Student t reference with 199 degrees of freedom. \*, \*\*, and \*\*\* denote unadjusted statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively

## 4.6 Summary of Findings

H1 is strongly supported. The cross-country difference remains significant after year fixed effects and firm-clustered standard errors are applied. Australian firms produce more informative cybersecurity-related disclosures than Chinese firms, and the difference holds across the aggregate score, each of the three dimensions, and most of the individual indicators. The gap also widens over the FY2022 to FY2024 period. The aggregate country difference also remains positive and statistically significant after broad sector fixed effects are included.

H2 receives no support at the aggregate CSRDS level. The aggregate CSRDS score and the three dimension-level measures remain insignificant after industry fixed effects are included. At the indicator level, R2 is negative and significant in the CAPM joint-indicator model, and it remains significant after Holm adjustment for multiple testing, both before and after industry adjustment. The supplementary separate-indicator CAPM R2 estimates do not meet the 5% threshold under the primary 18-test Holm adjustment. The R2 evidence should therefore be treated as supplementary indicator-level evidence, not as support for the aggregate H2 prediction.

H3 also receives no support. Neither the aggregate  $\text{CSRDS} \times \text{Australia}$  interaction nor the supplementary  $\text{R2} \times \text{Australia}$  interaction shows a statistically significant cross-country difference, and the aggregate H3 conclusion is unchanged after industry fixed effects are included.

The estimated indicator coefficients vary in sign and magnitude. The clearest indicator-level evidence appears for R2 in the CAPM joint-indicator model, but this finding is narrower than the aggregate H2 prediction and is not uniformly reproduced across alternative financing-cost and multiplicity-adjusted specifications.

## Chapter 5. Discussion and Implications

This chapter discusses the empirical findings in relation to the three hypotheses developed in Chapter 2. H1 is supported, as Australian firms provide more informative cybersecurity related disclosures than Chinese firms at the aggregate and dimension levels and across most individual indicators. H2 is not supported by the primary aggregate model because neither aggregate CSRDS nor the three dimension scores are significantly associated with the cost of equity. At the indicator level, R2, which is the Cyber risk and business consequences indicator, is negatively associated with the cost of equity in the CAPM joint-indicator model and remain statistically significant after the primary Holm multiple-testing adjustment. **This indicator-level result is treated as supplementary evidence and does not alter the conclusion that H2 is unsupported at the aggregate CSRDS level.**

The findings reveal a distinction between the production of informative cybersecurity disclosure and its association with the cost of equity. Institutional differences are more clearly reflected in what firms disclose than in cross-country variation in the association with the cost of equity. The results also suggest that aggregate disclosure informativeness should be distinguished from specific consequence-oriented content when assessing the economic relevance of cybersecurity reporting.

### 5.1 Institutional Environments and the Production of Informative Cybersecurity Disclosure

The first major finding supports H1. Australian firms provide more informative cybersecurity related disclosures than Chinese firms, and the difference appears in aggregate CSRDS and across the three dimensions of Specificity, Relevance, and Usefulness. The country difference therefore extends beyond the amount or simple presence of cyber related text. Rather, the results indicate that Australian firms are more likely to provide content that enables external users to assess particular cyber threats, preparedness mechanisms, exposures, and potential business consequences. The additional robustness test shows that the aggregate country difference remains positive and statistically significant after broad sector fixed effects are included, indicating that broad sector composition does not fully explain the H1 result.

Illustrative evidence from the coded annual reports helps clarify the nature of this difference. Energy One's FY2024 report identifies a ransomware incident and connects cyberattacks to potential downtime, system failure, service interruption, and data theft. Perpetual's FY2024 report discusses penetration testing, red team exercises, vulnerability management, response planning, business continuity, third-party technology due diligence, cyber insurance, and board oversight. In the selected Chinese examples, the reports of Quantum CTEK and 3onedata place greater emphasis on information security systems, certifications, legal compliance, data security policies, and management controls. These examples are illustrative rather than representative evidence by themselves, but they are consistent with the broader statistical pattern. The Australian advantage is more apparent in threat specific, control specific, and consequence-oriented disclosure than in the simple acknowledgement of cybersecurity as a reporting topic. This pattern is also consistent with cross-country disclosure research showing that national institutions are associated with the substance and informativeness of firm level reporting (Bushman et al., 2004; Leuz & Wysocki, 2016; Liu et al., 2024).

Institutional theory provides a useful framework for interpreting these differences. DiMaggio and Powell (1983) distinguish coercive pressure arising from laws, regulators, and exchange requirements, mimetic pressure arising from industry norms and peer practices, and normative pressure arising from professional expectations about appropriate corporate reporting. The present study does not measure these pressures separately, but they provide a framework for considering why firms operating in different national reporting environments may face different incentives to provide informative cybersecurity disclosure.

The central distinction is not that Australia regulates cybersecurity while China does not. Both countries have developed legal and regulatory frameworks relating to cybersecurity, data protection, and listed firm disclosure. The difference lies more in the relative orientation of the broader reporting environments. Australia's listed firm environment is relatively market-facing, combining continuous disclosure obligations for market sensitive information with governance expectations relating to the identification, management, and communication of material business risks (ASX Corporate Governance Council, 2019; ASX Limited, 2024). China's listed firm disclosure framework also includes investor protection objectives, but cybersecurity reporting is more visibly embedded within a

broader framework of compliance, data governance, regulatory administration, and state supervision (Barry et al., 2022; Creemers, 2024; Lu et al., 2023).

The coded examples are consistent with these relative orientations. The Australian examples are more directly framed around external user assessment and potential business consequences, while the selected Chinese examples place greater emphasis on compliance systems and internal controls. This does not imply that Chinese firms fail to disclose cybersecurity information or that all Australian disclosure is investor oriented. The observed difference concerns the dominant framing and informativeness of the reported content. This interpretation is consistent with broader risk disclosure research, which argues that disclosure quality depends not only on how much information is provided but also on its substance and presentation (Beretta & Bozzolan, 2004).

The indicator results provide further insight into the nature of the country difference. The Australian advantage is not uniform across all nine indicators. The largest differences occur for S1, Specific cyber threats, and R2, Cyber risk and business consequences. Australian firms also score significantly higher on S2, Cyber resilience and readiness, R3, Third-party and compliance cyber risks, and U2, Cyber insurance and exposure. This pattern indicates that Australian observations are more likely to identify particular threats, describe preparedness mechanisms, connect cyber risk to business consequences, and provide information about external exposure or risk transfer.

One interpretation is that the larger differences in S1 and R2 are consistent with the market-facing and governance related pressures present in the Australian reporting environment. Both indicators require firms to make relatively active and firm-specific judgements about the threats they face and the operational or financial consequences those threats may produce. However, the empirical models do not separately identify coercive, mimetic, or normative mechanisms. The indicator results should therefore be interpreted as consistent with institutional theory rather than as direct evidence that a particular institutional pressure caused the observed differences.

The absence of significant country differences for S3 and U1 provides an important qualification. S3 requires firms to identify critical digital assets, systems, or data resources, while U1 requires quantified information about cybersecurity expenditure, staffing, training, or other resources.

Disclosure in these areas may depend on internal asset mapping, information systems, measurement capacity, and willingness to disclose security sensitive information. Firms may also limit such detail when it could reveal sensitive systems, resource allocations, or potential vulnerabilities. These considerations may help explain why S3 and U1 show limited country variation despite the broader Australian advantage. This interpretation is consistent with proprietary cost and security sensitivity concerns in disclosure theory, under which firms may generalise or withhold information when greater specificity could reveal commercially sensitive or exploitable information (Hope et al., 2016; SEC, 2023; Verrecchia, 1983).

R1, Active cyber governance, also does not show a robust Australian advantage. Although the unadjusted comparison reports a marginally higher Chinese mean, the country difference is not statistically significant after standard errors are clustered by firm. This result indicates that formal governance and oversight language is not uniquely associated with the Australian reporting environment. It also reinforces the conclusion that the institutional pattern is selective rather than uniform across every disclosure attribute.

The widening aggregate CSRDS difference from FY2022 to FY2024 provides a final qualification. Australian scores increase over the sample period, while Chinese scores remain relatively stable. This temporal pattern is consistent with cybersecurity becoming more visible in Australian corporate reporting, but it should not be interpreted as causal evidence of a particular regulatory development or market event. The analysis does not identify which institutional change, if any, produced the observed increase.

Overall, H1 provides evidence that cybersecurity disclosure informativeness differs systematically between Australia and China. The pattern is consistent with institutional theory because country differences are most visible in disclosure attributes requiring firm-specific threat identification and explanation of business consequences. However, the results do not isolate the causal effect of any particular legal, regulatory, professional, or market mechanism. They show that institutional reporting environments are associated with the production and framing of cybersecurity disclosure, while the cost of equity implications of that disclosure require separate consideration under H2 and H3.

## 5.2 Business Consequence Disclosure and the Cost of Equity Association

The second major finding is that aggregate CSRDS is not significantly associated with the cost of equity, whereas R2, Cyber risk and business consequences, is the only indicator with a negative and statistically significant coefficient in the CAPM joint-indicator model. The R2 coefficient remains statistically significant in that joint model after Holm adjustment for multiple testing and after the inclusion of industry fixed effects. However, this adjusted inference is not uniform across the supplementary separate-indicator specification or the LSEG outcome. This pattern does not support H2 at the aggregate CSRDS level. Instead, R2 is interpreted as narrower, supplementary indicator-level evidence.

The non-significant aggregate result is theoretically informative because it is consistent with cybersecurity disclosure not having a single, uniform association with the cost of equity. Some disclosures may reduce information uncertainty by clarifying firm-specific cyber exposure, such as dependence on digital platforms, customer data, cloud services, payment systems, or third-party technology providers. Prior research similarly suggests that firm-specific risk disclosure can be more informative than generic risk language (Campbell et al., 2014; Hope et al., 2016; Leuz & Verrecchia, 2000). Other disclosures may primarily acknowledge the existence of cyber risk, describe governance arrangements, or report compliance processes. Detailed disclosure may also indicate greater underlying exposure, as prior cybersecurity research shows that disclosure can contain heterogeneous information about operations, vulnerabilities, controls, and subsequent incidents (Cheong et al., 2021; Gao et al., 2020; H. Li et al., 2018).

When these different disclosure attributes are combined into a single index, their associations may differ in direction or magnitude and may therefore attenuate or offset one another. Signal mixing is one possible interpretation of why aggregate CSRDS does not exhibit a significant negative association with the cost of equity. However, the present models do not directly identify this mechanism. The aggregate result could also reflect measurement limitations, statistical noise, or differences in how the underlying disclosure attributes relate to the cost of equity.

The R2 result qualifies the non-significant aggregate result by identifying one specific disclosure

attribute with a negative association. R2 measures whether firms connect cyber risk to potential operational or financial consequences through particular business processes. These consequences may include operational disruption, service interruption, regulatory exposure, customer related effects, and disruption to supply chains or other business relationships. The result therefore suggests that the cost of equity association is observed for disclosure that connects cyber risk to firm level business consequences rather than being distributed uniformly across the CSRDS construct.

The R2-specific result is consistent with the estimation risk mechanism developed in Chapter 2. Lambert et al. (2007) explain that uncertainty about the distribution of future cash flows can affect investors' required returns. In the cybersecurity setting, consequence-oriented disclosure may reduce part of this uncertainty by translating technical cyber risk into more assessable economic exposure. R2 provides this connection by explaining how a cyber event could affect operations, customers, regulatory obligations, or other sources of firm value.

Other indicators may still provide relevant information, but they do not necessarily connect cyber risk to expected economic consequences as directly as R2. For example, S1 may identify the types of cyber threats faced by the firm, while governance, compliance, insurance, and performance disclosures may provide information about how cyber risk is recognised or managed. These disclosures may be useful for other purposes, even though their coefficients are not statistically significant in the reported cost of equity model. R2 may nevertheless provide a more direct connection between technical cyber risk and potential economic consequences than the other indicators. Such information may help external users assess why cybersecurity risk matters economically for the firm.

This interpretation is consistent with risk disclosure research showing that firm-specific disclosure is generally more informative than generic risk language (Campbell et al., 2014; Hope et al., 2016). It is also consistent with cybersecurity disclosure research suggesting that market relevance depends on the substance of the information provided rather than disclosure presence or volume alone (Berkman et al., 2018; Gordon et al., 2010). One possible interpretation is therefore that the negative R2 association is consistent with lower estimation risk when disclosure translates technical cyber risk into assessable business consequences. The present analysis does not, however, directly test whether estimation risk is

the mechanism through which the association arises.

The R2 finding can also be compared with Havakhor et al. (2026), one of the relatively few studies directly linking cybersecurity disclosure to financing costs. Havakhor et al. examine cybersecurity investment disclosure, whereas the present study evaluates a broader annual report construct comprising nine indicators of disclosure informativeness. The disclosure categories are therefore different. Nevertheless, the two studies point to a related implication. Havakhor et al. find that the financing cost association is stronger when cybersecurity investment disclosure is less boilerplate and supported by underlying investment activity. In the present study, the negative cost of equity association is observed for R2, which connects cyber risk to assessable business consequences.

These findings motivate closer examination of concrete and economically interpretable cybersecurity disclosure attributes when studying financing-cost associations. In the present study, the R2 result also illustrates the analytical value of disaggregating the composite CSRDS measure, because the aggregate score and the individual disclosure attributes do not exhibit uniform associations with the cost of equity.

### **5.3 Institutional Context and Cross-country Variation in the Cost of Equity Association**

The third finding extends the institutional comparison from cross-country differences in disclosure informativeness to cross-country differences in its association with the cost of equity. While H1 examines whether Australian firms provide more informative CSRDS than Chinese firms, H3 examines whether the association between CSRDS and the cost of equity is stronger in Australia. This distinction matters because institutional differences may be reflected in disclosure production without necessarily being reflected in stronger cost of equity associations. In other words, disclosure production and disclosure pricing are related but not the same mechanism.

The formal interaction results do not support H3. Neither the aggregate CSRDS  $\times$  Australia interaction nor the supplementary R2  $\times$  Australia interaction is statistically significant. This means that the evidence does not show a stronger CSRDS and cost of equity association in Australia, even though Australian firms provide more informative CSRDS on average. This result separates the supply of

disclosure from the pricing of disclosure. The H1 evidence shows that Australia's institutional environment is associated with more informative CSRDS, but the H3 evidence shows that this disclosure advantage does not automatically translate into a stronger market-pricing effect.

The Australian R2 subsample result still provides useful supplementary insight. It is directionally consistent with the argument that consequence-oriented disclosure may have a stronger association with the cost of equity in a market-facing reporting environment. However, because the formal  $R^2 \times \text{Australia}$  interaction is not statistically significant, this subsample evidence is best interpreted as suggestive rather than as formal moderation evidence.

One possible explanation for the non-significant H3 result is that the institutional channels developed in Chapter 2 operate in competing directions. Based on the credibility and investor-processing channels, a stronger negative relationship between CSRDS and the cost of equity would be expected in Australia. Australia's more market-facing reporting environment may make firm-specific CSRDS more credible and more likely to be processed by investors and information intermediaries (Hail & Leuz, 2006; Blankespoor et al., 2020). However, this prediction is complicated by the information-environment channel. Because Australia has a richer surrounding information environment, some cyber-related information may already be communicated through continuous disclosure, analyst coverage, market announcements, media reporting, or other firm-specific information channels (Beyer et al., 2010; Healy & Palepu, 2001). Conversely, in China, where public disclosure practices are shaped by distinctive institutional arrangements and private communication channels, standardised annual-report CSRDS may still provide useful public information when it conveys firm-specific cybersecurity awareness (Barry et al., 2022; Lu et al., 2023). These opposing forces may partly offset each other, helping to explain why the formal interaction terms are not statistically significant.

A further possible explanation for the insignificant aggregate interaction is the signal mixing problem identified in the H2 analysis. Since the aggregate CSRDS index combines various disclosure attributes that may have heterogeneous associations with the cost of equity across countries, this aggregation may attenuate the estimated slopes for both Australia and China, thereby diminishing the observable

cross-country difference. However, this explanation does not extend to the  $R2 \times \text{Australia}$  interaction, as  $R2$  is estimated as a separate, standalone indicator. The non-significant  $R2$  interaction does not provide evidence that the association differs between Australia and China.

Overall, the  $H3$  results indicate that institutional differences are more clearly reflected in the production and framing of CSRDS than in cross-country variation in its association with the cost of equity. Neither the aggregate CSRDS interaction nor the  $R2$  interaction is statistically significant. Therefore, the evidence does not establish that the association between CSRDS informativeness and the cost of equity is stronger in Australia than in China. Accordingly,  $H3$  is not supported, although the Australian subsample result indicates that the negative  $R2$  association is more evident among Australian firms.

## **5.4 Contributions and Practical Implications**

### **5.4.1 Research Contributions**

This study makes three main contributions to the cybersecurity disclosure, risk disclosure, and cross-country accounting literature.

First, the study extends cybersecurity disclosure research beyond the predominantly United States centred capital-market setting by providing comparative evidence from Australia and China. Although prior cybersecurity disclosure research is not confined to the United States, the literature remains strongly influenced by SEC filings, cyber incident data, and United States capital-market evidence (Amani et al., 2025). The present study examines listed firms under their respective domestic reporting and regulatory environments rather than comparing firms within a common SEC reporting framework.

The  $H1$  results show that Australian firms provide more informative cybersecurity related disclosures than Chinese firms, particularly for attributes involving specific threats and business consequences. The contribution therefore lies not merely in documenting whether cyber related text appears in annual reports, but in showing that the substance and informativeness of disclosure differ across two domestic reporting environments. This finding extends cross-country disclosure research by demonstrating the relevance of institutional context to the content and framing of cybersecurity reporting, while not

attributing the observed country differences to any single regulatory mechanism.

Second, the study contributes to the measurement of cybersecurity disclosure informativeness. Rather than relying only on binary disclosure indicators, keyword frequency, disclosure length, or broad textual exposure (Berkman et al., 2018; Gao et al., 2020; H. Li et al., 2018), the thesis develops a codebook based CSRDS measure structured around Specificity, Relevance, and Usefulness. The nine indicator framework distinguishes among specific threat identification, cyber resilience, critical asset exposure, active governance, business consequences, third-party and compliance risks, quantified resources, cyber insurance, and measurable performance outcomes.

This multidimensional structure enables cybersecurity disclosure to be examined at the aggregate, dimension, and indicator levels. The contrast between the insignificant aggregate result and the more specific R2 evidence illustrates the analytical usefulness of examining underlying disclosure attributes alongside the composite score. The bilingual application of the framework also provides a structured basis for comparing English and Chinese annual report disclosures using common conceptual and scoring criteria.

Third, the study contributes to understanding the association between cybersecurity disclosure content and the cost of equity. The primary aggregate analysis does not support the predicted negative association between overall CSRDS informativeness and the cost of equity. At the indicator level, R2, Cyber risk and business consequences, has a negative and statistically significant coefficient in the CAPM joint-indicator model and remains significant after the primary Holm multiple-testing adjustment and the inclusion of industry fixed effects. However, this adjusted evidence is not uniform across the supplementary separate-indicator and LSEG specifications.

The contribution lies in showing that the aggregate CSRDS result and the underlying indicator-level associations are not uniform, with the clearest supplementary cost-of-equity evidence concerning business-consequence disclosure in the CAPM joint-indicator specification. This finding motivates closer examination of individual disclosure attributes alongside aggregate measures of cybersecurity disclosure informativeness. The analysis does not directly establish that investors process R2 disclosure through an information risk mechanism, but the result is consistent with the argument that

economically interpretable information may reduce uncertainty about firm-specific cyber exposure (Lambert et al., 2007; Leuz & Verrecchia, 2000).

#### **5.4.2 Practical Implications**

The findings also have practical implications for listed firms, regulators, standard setters, investors, and analysts. The central practical implication is that cybersecurity disclosure should not be assessed solely according to whether it is present or how much text is provided. Greater attention should be paid to consequence-oriented disclosure, particularly where it explains how cybersecurity risk could affect the firm's operations, cash flows, regulatory exposure, customer relationships, or supply-chain continuity.

For listed firms, generic statements about cyberattacks, controls, governance, or risk management may provide limited insight into the economic significance of cyber risk. Firms seeking more specific, consequence-oriented reporting could identify the relevant business areas and explain the potential operational, regulatory, customer-related, or financial consequences. This does not require disclosing sensitive technical details, system configurations, or information that could increase security exposure. Instead, firms can connect cyber risk to business implications that external users can assess while maintaining confidentiality over technical security information. These findings thus motivate greater attention to consequence-oriented disclosure alongside other characteristics of cybersecurity reporting.

For regulators and standard setters, the findings suggest that disclosure guidance could place greater emphasis on the connection between cybersecurity governance, controls, incident response, and firm-specific business consequences. Guidance could encourage firms to explain why a cyber risk or control matters to operations and financial exposure, rather than requiring more general cyber-related text. Any such guidance should remain sensitive to proprietary costs, security concerns, and differences in firms' business models and risk profiles.

For investors and analysts, the presence or volume of cybersecurity disclosure should not be treated as evidence of lower risk or greater transparency. More extensive disclosure may reflect better communication, but it may also indicate greater cyber exposure, prior incidents, or stronger regulatory

pressure. Because aggregate disclosure can contain both uncertainty-reducing and risk-revealing information, assessments should focus on whether firms link cybersecurity risk to identifiable business consequences alongside the presence and extent of cybersecurity disclosure.

## Chapter 6. Conclusion, Limitations, and Future Research

Cybersecurity risk has become an important corporate reporting and capital-market issue. As firms increasingly rely on digital infrastructure, data-intensive operations, and interconnected business processes, cybersecurity is no longer solely a technical concern. It has become a material business risk that investors may need to consider when assessing firm value, uncertainty, and financing costs. Against this background, this study examines the informativeness of cybersecurity-related disclosures in Australia and China using 600 firm-year observations covering FY2022 to FY2024.

Australian firms provide significantly more informative cybersecurity disclosures than Chinese firms, and the aggregate country difference remains statistically significant after broad industry adjustment. However, the capital-market evidence is more selective. Aggregate CSRDS and its three dimensions are not significantly associated with the cost of equity, even after industry fixed effects are included. At the indicator level, R2 is negatively associated with the cost of equity in the CAPM joint-indicator model and remains statistically significant after the primary Holm multiple-testing adjustment, both before and after industry adjustment. This Holm-adjusted evidence is not uniform across the supplementary separate-indicator or LSEG specifications. Turning to H3, neither the aggregate CSRDS interaction nor the R2 interaction provides support for H3.

Cross-country differences thus appear more clearly in the production of informative cybersecurity disclosure than in its cost-of-equity associations.

The following limitations define the scope of these findings and provide directions for future research.

**CSRDS Measurement.** The first limitation relates to the measurement of CSRDS. This study uses a structured codebook and rule-based scoring approach to improve consistency across 600 firm-year observations. This approach allows the analysis to compare disclosure informativeness across countries, dimensions, and indicators. However, cybersecurity disclosure is context-dependent, and some judgement is still required when assessing whether a disclosure is specific, relevant, or useful. Although the scoring rules were calibrated and validated, the validation reflects machine-human agreement after rule refinement rather than conventional blind double-coding by independent human

coders. The scoring approach may also not fully capture subtle differences in tone, emphasis, managerial intent, or the broader narrative context of the annual report. In addition, a zero CSRDS score can reflect either the absence of cybersecurity-related disclosure or the presence of cyber-related text that does not meet the minimum informativeness threshold. Future research could extend this measurement approach by combining rule-based scoring with additional manual coding, expert assessment, or more advanced textual analysis to capture more nuanced aspects of cybersecurity disclosure quality.

**Annual Reports as a Single Disclosure Channel.** Another limitation is that this study focuses on cybersecurity-related disclosure in annual reports. Annual reports are important formal reporting documents, but they are not the only channel through which firms communicate cybersecurity information. Firms may also disclose cybersecurity matters through continuous disclosure announcements, sustainability reports, corporate governance statements, investor presentations, websites, media releases, or regulatory filings. Therefore, the CSRDS measure in this study captures the informativeness of annual-report disclosure rather than the full cybersecurity information environment surrounding each firm. Future research could examine multiple disclosure channels to assess whether annual reports, market announcements, sustainability reports, or other communications provide different types of cybersecurity information.

**Disclosure Informativeness and Underlying Cyber Risk Exposure.** Additionally, this study cannot directly determine whether more informative cybersecurity disclosure reflects stronger cybersecurity preparedness or higher underlying cyber-risk exposure. More informative disclosure may indicate greater transparency, but it may also be provided by firms facing higher cyber exposure, stronger regulatory attention, or greater pressure to explain cyber-related risks. This issue is particularly important because external users cannot directly observe a firm's internal cybersecurity maturity, control quality, incident response capability, or risk exposure. Future research could combine disclosure data with cyber incident records, cybersecurity investment data, internal governance information, assurance reports, or third-party cyber-risk ratings to examine whether informative disclosure reflects better cybersecurity capability, greater exposure, or both.

**Causal Interpretation and Indicator-Level Evidence.** A further limitation concerns causal interpretation. The R2 result provides evidence of a negative association between business-consequence cybersecurity disclosure and the cost of equity, but the observational research design does not establish a causal effect. Firms with stronger R2 disclosure may differ from other firms in unobserved ways, such as cybersecurity maturity, internal control quality, governance capacity, risk-management culture, or investor-relations capability. Omitted correlated firm characteristics, disclosure self-selection, and reverse causality therefore remain possible. Accordingly, the research design does not resolve potential reverse causality or endogeneity. The H2 estimates and the supplementary R2 finding are therefore interpreted as associations rather than causal effects.

Because the indicator-level analysis examines nine related disclosure attributes, the R2 result serves as supplementary indicator-level evidence rather than confirmation of the aggregate H2 prediction. Future research could use event-based designs, regulatory changes, cyber incident shocks, or more detailed firm-level cybersecurity governance data to provide stronger evidence on whether business-consequence disclosure affects financing costs.

**Cost of Equity and Financing Cost Measurement.** The main analysis estimates the cost of equity using the CAPM, based on firm level beta and country year risk free rate and equity risk premium inputs. The robustness analysis uses LSEG StarMine WACC as an alternative market based financing cost outcome that incorporates capital structure considerations and a broader range of financing costs. These measures provide complementary perspectives on the association between CSRDS and financing costs, although both depend on model based inputs and estimation choices. Future research could extend the analysis using alternative implied cost of equity models, analyst forecast based measures, bond yield based measures, or market based proxies for information asymmetry, such as bid ask spreads and share liquidity.

**Scope and Generalisability.** The balanced sample of 100 firms per country also prioritises cross-country comparability over full population coverage. As a result, the design may provide lower statistical power for detecting smaller associations than a substantially larger sample and limits the extent to which the estimates can be generalised to the full eligible firm populations within Australia

and China. The cross-country design is limited to Australia and China over the FY2022 to FY2024 period. This setting is appropriate for examining two distinct institutional environments, but the findings should not be automatically generalised to all countries or periods. The Australia-China difference may reflect a combination of regulatory orientation, market structure, investor demand, reporting culture, industry composition, language, and broader information environments. The study also does not directly test the causal effect of any specific regulatory change during the sample period. Future research could extend the analysis to a larger set of countries, longer time periods, or settings with identifiable regulatory shocks. It could also examine other capital-market outcomes, such as analyst forecast accuracy, analyst following, bid-ask spreads, institutional ownership, stock price crash risk, or market reactions to cybersecurity incidents. Such research would help clarify when cybersecurity disclosure is merely present, when it is informative, and when it becomes economically useful.

The cross-country comparison shows that differences in institutional reporting environments are more clearly reflected in the production of informative cybersecurity disclosure than in its association with the cost of equity. The clearest supplementary cost-of-equity evidence concerns disclosures that connect cyber risk to potential business consequences in the CAPM joint-indicator specification, while the aggregate CSRDS evidence does not support H2. This distinction motivates further examination of individual disclosure attributes alongside aggregate disclosure measures.

By distinguishing aggregate scores from individual disclosure attributes and disclosure presence from disclosure informativeness, this thesis provides a more precise foundation for evaluating cybersecurity reporting. Although the findings are subject to limitations relating to measurement, disclosure channels, causal interpretation, financing cost measures, and generalisability, these limitations also identify clear priorities for future research.

## References

- Adam-Müller, A. F. A., & Erkens, M. H. R. (2020). Risk disclosure noncompliance. *Journal of Accounting and Public Policy*, 39(3), Article 106739. <https://doi.org/10.1016/j.jaccpubpol.2020.106739>
- Adams, M., & Moore, T. (2025). How informative are cybersecurity risk disclosures? Empirical analysis of firms targeted by ransomware. *Computers & Security*, 159, Article 104626. <https://doi.org/10.1016/j.cose.2025.104626>
- Ajina, A., Laouiti, M., & Msolli, B. (2016). Guiding through the fog: Does annual report readability reveal earnings management? *Research in International Business and Finance*, 38, 509–516. <https://doi.org/10.1016/j.ribaf.2016.07.021>
- Akerlof, G. A. (1970). The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3), 488–500. <https://doi.org/10.2307/1879431>
- Al Amosh, H., & Khatib, S. F. A. (2025). Cybersecurity transparency and firm success: Insights from the Australian landscape. *Australian Economic Papers*, 64(2), 189–204. <https://doi.org/10.1111/1467-8454.12385>
- Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors’ confidence: The context of efficient market hypothesis. *Sustainability*, 13(3), Article 1066. <https://doi.org/10.3390/su13031066>
- Allen, F., Qian, J., & Qian, M. (2005). Law, finance, and economic growth in China. *Journal of Financial Economics*, 77(1), 57–116. <https://doi.org/10.1016/j.jfineco.2004.06.010>
- Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives*, 24(3), 605–667. <https://doi.org/10.1111/1911-3838.12411>
- Amihud, Y. (2002). Illiquidity and stock returns: Cross-section and time-series effects. *Journal of Financial Markets*, 5(1), 31–56. [https://doi.org/10.1016/S1386-4181\(01\)00024-6](https://doi.org/10.1016/S1386-4181(01)00024-6)
- Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), 1177–1206. <https://doi.org/10.1007/s11142-018-9452-4>
- Andrew, J., Baker, M., Wang, X., & Sheehan, M. (2026). Exploring the materiality of data breach

- disclosures on the Australian Stock Exchange. *Abacus*, 62(3), 673–697.  
<https://doi.org/10.1111/abac.70001>
- Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, 98(4), 1–32.  
<https://doi.org/10.2308/TAR-2020-0787>
- ASX Corporate Governance Council. (2019). *Corporate governance principles and recommendations* (4th ed.). ASX Limited.  
<https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf>
- ASX Limited. (2023). *ASX submission to continuous disclosure: Review of changes made by the Treasury Laws Amendment (2021 Measures No. 1) Act 2021*.  
<https://www2.asx.com.au/content/dam/asx/about/regulations/public-consultations/2023/asx-submission-review-of-changes-to-continuous-disclosure-20231208.pdf>
- ASX Limited. (2024). *Guidance note 8: Continuous disclosure: Listing Rules 3.1–3.1B*.  
<https://www.asx.com.au/content/dam/asx/rules-guidance-notes-waivers/asx-listing-rules/guidance-notes/gn08-continuous-disclosure.pdf>
- Australian Government. (2024). *Government response to the report of the independent review of the changes to the continuous disclosure laws*. The Treasury.  
<https://treasury.gov.au/publication/p2024-561348>
- Australian Prudential Regulation Authority. (2019). *Prudential standard CPS 234: Information security*.  
[https://www.apra.gov.au/sites/default/files/cps\\_234\\_july\\_2019\\_for\\_public\\_release.pdf](https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf)
- Australian Securities and Investments Commission. (n.d.). *Handling corporate information*.  
<https://www.asic.gov.au/regulatory-resources/corporate-governance/handling-corporate-information/>
- Australian Securities and Investments Commission. (2017). *Regulatory guide 73: Continuous disclosure obligations: Infringement notices*.  
<https://download.asic.gov.au/media/1htl4i4p/rg73-published-31-october-2017-20230705.pdf>
- Australian Securities and Investments Commission. (2022, July 15). *Cyber risk: Be prepared*.  
<https://asic.gov.au/about-asic/news-centre/articles/cyber-risk-be-prepared/>

- Australian Securities and Investments Commission. (2025, June 4). *Here to stay, here to grow: The future of Australia's public and private markets*. <https://www.asic.gov.au/about-asic/news-centre/speeches/here-to-stay-here-to-grow-the-future-of-australia-s-public-and-private-markets/>
- Bansal, G., & Axelton, Z. (2024). Impact of cybersecurity disclosures on stakeholder intentions. *Journal of Computer Information Systems*, 64(1), 78–91. <https://doi.org/10.1080/08874417.2023.2180785>
- Barry, C. B., & Brown, S. J. (1985). Differential information and security market equilibrium. *Journal of Financial and Quantitative Analysis*, 20(4), 407–422. <https://doi.org/10.2307/2330758>
- Barry, T., Jona, J., & Soderstrom, N. S. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy*, 41(6), Article 106998. <https://doi.org/10.1016/j.jaccpubpol.2022.106998>
- Beattie, V., McInnes, B., & Fearnley, S. (2004). A methodology for analysing and evaluating narratives in annual reports: A comprehensive descriptive profile and metrics for disclosure quality attributes. *Accounting Forum*, 28(3), 205–236. <https://doi.org/10.1016/j.accfor.2004.07.001>
- Beretta, S., & Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *The International Journal of Accounting*, 39(3), 265–288. <https://doi.org/10.1016/j.intacc.2004.06.006>
- Beretta, S., & Bozzolan, S. (2008). Quality versus quantity: The case of forward-looking disclosure. *Journal of Accounting, Auditing & Finance*, 23(3), 333–376. <https://doi.org/10.1177/0148558X0802300304>
- Berkman, H., Jona, J., Lee, G., & Soderstrom, N. S. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508–526. <https://doi.org/10.1016/j.jaccpubpol.2018.10.003>
- Berkman, H., Jona, J., Lee, G., & Soderstrom, N. S. (2021). *Digital insiders and informed trading before earnings announcements*. SSRN. <https://doi.org/10.2139/ssrn.3180531>
- Beyer, A., Cohen, D. A., Lys, T. Z., & Walther, B. R. (2010). The financial reporting environment: Review of the recent literature. *Journal of Accounting and Economics*, 50(2–3), 296–343. <https://doi.org/10.1016/j.jacceco.2010.10.003>

- Blankespoor, E., deHaan, E., & Marinovic, I. (2020). Disclosure processing costs, investors' information choice, and equity market outcomes: A review. *Journal of Accounting and Economics*, 70(2–3), Article 101344. <https://doi.org/10.1016/j.jacceco.2020.101344>
- Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly*, 43(1), 313–327. <https://doi.org/10.25300/MISQ/2019/14192>
- Botosan, C. A. (1997). Disclosure level and the cost of equity capital. *The Accounting Review*, 72(3), 323–349.
- Botosan, C. A., & Plumlee, M. A. (2002). A re-examination of disclosure level and the expected cost of equity capital. *Journal of Accounting Research*, 40(1), 21–40. <https://doi.org/10.1111/1475-679X.00037>
- Bowen, R. M., Chen, X., & Cheng, Q. (2008). Analyst coverage and the cost of raising equity capital: Evidence from underpricing of seasoned equity offerings. *Contemporary Accounting Research*, 25(3), 657–700. <https://doi.org/10.1506/car.25.3.1>
- Brockman, P., Gao, X., Li, X., & Xu, Y. (2023). The impact of differential risk disclosures: Evidence from cross-listed firms in China and Hong Kong. *International Review of Economics & Finance*, 88, 442–457. <https://doi.org/10.1016/j.iref.2023.06.026>
- Brunnermeier, M. K., Sockin, M., & Xiong, W. (2022). China's model of managing the financial system. *The Review of Economic Studies*, 89(6), 3115–3153. <https://doi.org/10.1093/restud/rdab098>
- Bushman, R. M., Piotroski, J. D., & Smith, A. J. (2004). What determines corporate transparency? *Journal of Accounting Research*, 42(2), 207–252. <https://doi.org/10.1111/j.1475-679X.2004.00136.x>
- Calderon, T. G., & Gao, L. (2022). Comparing the cybersecurity risk disclosures of U.S. and foreign firms. *Journal of Emerging Technologies in Accounting*, 19(2), 61–79. <https://doi.org/10.2308/JETA-2020-008>
- Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H.-M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, 19(1), 396–455. <https://doi.org/10.1007/s11142-013-9258-3>
- Cao, F., Xuan, Y., Yuan, R., & Zou, H. (2025). Governance by one-lot shares. *Journal of Financial*

- and *Quantitative Analysis*, 60(2), 874–909. <https://doi.org/10.1017/S0022109024000516>
- Cao, N., McGuinness, P. B., & Xi, C. (2021). Does securities enforcement improve disclosure quality? An examination of Chinese listed companies' restatement activities. *Journal of Corporate Finance*, 67, Article 101877. <https://doi.org/10.1016/j.jcorpfin.2020.101877>
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 70–104. <https://doi.org/10.1080/10864415.2004.11044320>
- Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, 50(4), 651–661. <https://doi.org/10.1016/j.dss.2010.08.017>
- Chang, K.-C., Gao, Y.-K., & Lee, S.-C. (2020). The effect of data theft on a firm's short-term and long-term market value. *Mathematics*, 8(5), Article 808. <https://doi.org/10.3390/math8050808>
- Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187(1), 199–224. <https://doi.org/10.1007/s10551-022-05107-z>
- Chen, X. C., Choi, K. W., Wright, S., & Wu, H. (2023). The effectiveness of sanctions on disclosure regulation: Australian evidence. *Accounting & Finance*, 63(4), 3841–3872. <https://doi.org/10.1111/acfi.13073>
- Chen, Y., Yuan, W., & Li, Z. (2021). Jianguanxing xiaogudong xingquan de youxiaoxing yanjiu: Jiyu toufu zhongxin de jingyan zhengju [Effectiveness of regulatory minority shareholders exercising rights: Evidence from the China Securities Investor Services Center]. *Guanli Shijie [Management World]*, 37(6), 142–158. <https://doi.org/10.3969/j.issn.1002-5502.2021.06.027>
- Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, 35(2), 179–194. <https://doi.org/10.2308/ISYS-2020-031>
- China Securities Regulatory Commission. (2021a, March 18). *Shangshi gongsi xinxi pilu guanli banfa* [Measures for the administration of information disclosure by listed companies] (CSRC Order No. 182). <https://www.csrc.gov.cn/csrc/c101864/c2ee1a791fddc4f5ebee70aa8e2399cf/content.shtml>

- China Securities Regulatory Commission. (2021b, June 28). *Gongkai faxing zhengquan de gongsi xinxi pilu neirong yu geshi zhunze di 2 hao—Niandu baogao de neirong yu geshi (2021 nian xiuding)* [Standards for the contents and formats of information disclosure by companies offering securities to the public No. 2—Contents and formats of annual reports (2021 revision)].  
<https://www.csrc.gov.cn/csrc/c101864/c6df1268b5b294448bdec7e010d880a01/content.shtml>
- Chordia, T., Roll, R., & Subrahmanyam, A. (2001). Market liquidity and trading activity. *The Journal of Finance*, 56(2), 501–530. <https://doi.org/10.1111/0022-1082.00335>
- Creemers, R. (2024). The Chinese conception of cybersecurity: A conceptual, institutional, and regulatory genealogy. *Journal of Contemporary China*, 33(146), 173–188. <https://doi.org/10.1080/10670564.2023.2196508>
- Cybersecurity and Infrastructure Security Agency. (2020). *Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations* (Alert AA20-352A). <https://content.govdelivery.com/accounts/USDHSCISA/bulletins/2b1b32d>
- Damodaran, A. (2022). *Country default spreads and risk premiums* [Data set]. Stern School of Business, New York University. [https://pages.stern.nyu.edu/~adamodar/New\\_Home\\_Page/dataarchived.html](https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html)
- Damodaran, A. (2023). *Country default spreads and risk premiums* [Data set]. Stern School of Business, New York University. [https://pages.stern.nyu.edu/~adamodar/New\\_Home\\_Page/dataarchived.html](https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html)
- Damodaran, A. (2024). *Country default spreads and risk premiums* [Data set]. Stern School of Business, New York University. [https://pages.stern.nyu.edu/~adamodar/New\\_Home\\_Page/dataarchived.html](https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html)
- Dang, T. V., Li, W., & Wang, Y. (2024). Government stock purchase undermines price informativeness: Evidence from China’s “National Team.” *Journal of Financial and Quantitative Analysis*, 59(5), 2340–2374. <https://doi.org/10.1017/S0022109023000637>
- da Silva, P. P. (2025). Non-financial disclosure and stock price informativeness: The role of country-level institutional factors. *Financial Markets and Portfolio Management*, 39, 225–258. <https://doi.org/10.1007/s11408-025-00466-9>
- Depoers, F., & Jérôme, T. (2020). Coercive, normative, and mimetic isomorphisms as drivers of corporate tax disclosure: The case of the tax reconciliation. *Journal of Applied Accounting*

*Research*, 21(1), 90–105. <https://doi.org/10.1108/JAAR-04-2018-0048>

- Dhaliwal, D. S., Li, O. Z., Tsang, A., & Yang, Y. G. (2011). Voluntary nonfinancial disclosure and the cost of equity capital: The initiation of corporate social responsibility reporting. *The Accounting Review*, 86(1), 59–100. <https://doi.org/10.2308/accr.00000005>
- Diamond, D. W., & Verrecchia, R. E. (1991). Disclosure, liquidity, and the cost of capital. *The Journal of Finance*, 46(4), 1325–1359. <https://doi.org/10.1111/j.1540-6261.1991.tb04620.x>
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Easley, D., & O'Hara, M. (2004). Information and the cost of capital. *The Journal of Finance*, 59(4), 1553–1583. <https://doi.org/10.1111/j.1540-6261.2004.00672.x>
- Elmawazini, K., Saadi, S., Sassi, S., Khiyar, K. A., & Ali, M. (2023). Do data breach disclosure laws matter to shareholder risk? *Finance Research Letters*, 53, Article 103588. <https://doi.org/10.1016/j.frl.2022.103588>
- Equifax Inc. (2017, September 7). *Equifax announces cybersecurity incident involving consumer information* [Press release]. <https://investor.equifax.com/news-events/press-releases/detail/240/equifax-announces-cybersecurity-incident-involving-consumer>
- Equifax Inc. (2018). *2017 annual report*. [https://d1io3yog0oux5.cloudfront.net/\\_f100f6fe54b5448270c3d9b20197add1/equifax/db/2054/18645/annual\\_report/2017-annual-report.pdf](https://d1io3yog0oux5.cloudfront.net/_f100f6fe54b5448270c3d9b20197add1/equifax/db/2054/18645/annual_report/2017-annual-report.pdf)
- European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- Fama, E. F., & French, K. R. (1992). The cross-section of expected stock returns. *The Journal of Finance*, 47(2), 427–465. <https://doi.org/10.1111/j.1540-6261.1992.tb04398.x>
- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, 36(1), 351–407. <https://doi.org/10.1093/rfs/hhac024>

- Fortin, A., & Héroux, S. (2023). Limited usefulness of firm-provided cybersecurity information in institutional investors' investment analysis. *Information and Computer Security*, 31(1), 108–123. <https://doi.org/10.1108/ICS-07-2022-0122>
- Francis, J., LaFond, R., Olsson, P. M., & Schipper, K. (2004). Costs of equity and earnings attributes. *The Accounting Review*, 79(4), 967–1010. <https://doi.org/10.2308/accr.2004.79.4.967>
- Francis, J. R., Khurana, I. K., & Pereira, R. (2005). Disclosure incentives and effects on cost of capital around the world. *The Accounting Review*, 80(4), 1125–1162. <https://doi.org/10.2308/accr.2005.80.4.1125>
- Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy*, 54, Article 107376. <https://doi.org/10.1016/j.jaccpubpol.2025.107376>
- Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 38, Article 100468. <https://doi.org/10.1016/j.accinf.2020.100468>
- Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, 89(3), 725–763. <https://doi.org/10.1111/jori.12381>
- Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, 13(1), 61–83. <https://doi.org/10.1111/j.1540-6296.2010.01178.x>
- Gauch, K., & Quick, R. (2025). Assure or insure cyber risk? Nonprofessional investors' willingness to invest. *Accounting Perspectives*, 24(2), 517–552. <https://doi.org/10.1111/1911-3838.12389>
- Gebhardt, W. R., Lee, C. M. C., & Swaminathan, B. (2001). Toward an implied cost of capital. *Journal of Accounting Research*, 39(1), 135–176. <https://doi.org/10.1111/1475-679X.00007>
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3), 567–594. <https://doi.org/10.2307/25750692>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33–56. <https://doi.org/10.3233/JCS-2009-0398>

- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808–834. <https://doi.org/10.1108/MAJ-09-2018-2004>
- Hail, L. (2002). The impact of voluntary corporate disclosures on the ex-ante cost of capital for Swiss firms. *European Accounting Review*, 11(4), 741–773. <https://doi.org/10.1080/0963818022000001109>
- Hail, L., & Leuz, C. (2006). International differences in the cost of equity capital: Do legal institutions and securities regulation matter? *Journal of Accounting Research*, 44(3), 485–531. <https://doi.org/10.1111/j.1475-679X.2006.00209.x>
- Harris, D., Kuzey, C., Naaman, C., & Sahyoun, N. (2023). Cybersecurity risk disclosure quality: Does it affect the cost of debt? *Journal of Forensic and Investigative Accounting*, 15(2), 192–212.
- Havakhor, T., Rahman, M. S., & Zhang, T. (2026). Disclosure of cybersecurity investments and the cost of capital. *Information Systems Research*, 37(3), 1782–1804. <https://doi.org/10.1287/isre.2023.0260>
- Hayn, C. (1995). The information content of losses. *Journal of Accounting and Economics*, 20(2), 125–153. [https://doi.org/10.1016/0165-4101\(95\)00397-2](https://doi.org/10.1016/0165-4101(95)00397-2)
- Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, 31(1–3), 405–440. [https://doi.org/10.1016/S0165-4101\(01\)00018-0](https://doi.org/10.1016/S0165-4101(01)00018-0)
- Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares?* (Georgetown McDonough School of Business Research Paper No. 2852519). SSRN. <https://doi.org/10.2139/ssrn.2852519>
- Hogan, K. M., Olson, G. T., Mills, J. D., & Zaleski, P. A. (2023). An analysis of cyber breaches and effects on shareholder wealth. *International Journal of the Economics of Business*, 30(1), 51–78. <https://doi.org/10.1080/13571516.2023.2168994>
- Hooks, J., & van Staden, C. J. (2011). Evaluating environmental disclosures: The relationship between quality and extent measures. *The British Accounting Review*, 43(3), 200–213. <https://doi.org/10.1016/j.bar.2011.06.005>
- Hope, O.-K. (2003a). Disclosure practices, enforcement of accounting standards, and analysts' forecast accuracy: An international study. *Journal of Accounting Research*, 41(2), 235–272. <https://doi.org/10.1111/1475-679X.00102>

- Hope, O.-K. (2003b). Firm-level disclosures and the relative roles of culture and legal origin. *Journal of International Financial Management & Accounting*, 14(3), 218–248. <https://doi.org/10.1111/1467-646X.00097>
- Hope, O.-K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies*, 21(4), 1005–1045. <https://doi.org/10.1007/s11142-016-9371-1>
- House of Representatives Standing Committee on Economics. (2022). *Report on the implications of common ownership and capital concentration in Australia*. Parliament of Australia. [https://www.aph.gov.au/Parliamentary\\_Business/Committees/House/Economics/~/\\_link.aspx?\\_id=8284658EEE5C41DBBFAEDA854C32546D](https://www.aph.gov.au/Parliamentary_Business/Committees/House/Economics/~/_link.aspx?_id=8284658EEE5C41DBBFAEDA854C32546D)
- Huang, A. H., Lehavy, R., Zang, A. Y., & Zheng, R. (2018). Analyst information discovery and interpretation roles: A topic modeling approach. *Management Science*, 64(6), 2833–2855. <https://doi.org/10.1287/mnsc.2017.2751>
- Huang, J. A., & Murthy, U. (2024). The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions. *International Journal of Accounting Information Systems*, 54, Article 100696. <https://doi.org/10.1016/j.accinf.2024.100696>
- Ibrahim, A. E. A., Hussainey, K., Nawaz, T., Ntim, C., & Elamer, A. A. (2022). A systematic literature review on risk disclosure research: State-of-the-art and future research agenda. *International Review of Financial Analysis*, 82, Article 102217. <https://doi.org/10.1016/j.irfa.2022.102217>
- IFRS Foundation. (2024, February). *Using SASB Standards to meet the requirements in IFRS S1*. <https://www.ifrs.org/content/dam/ifrs/supporting-implementation/ifrs-s1/using-sasb-standards-for-ifrs-s1.pdf>
- International Accounting Standards Board. (2018). *Conceptual framework for financial reporting*. IFRS Foundation. <https://www.ifrs.org/projects/completed-projects/2018/conceptual-framework/>
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. <https://www.iso.org/standard/27001>
- Jamilov, R., Rey, H., & Tahoun, A. (2023). *The anatomy of cyber risk* (INET Working Paper No. 206). Institute for New Economic Thinking. <https://doi.org/10.36687/inetwp206>

- Jiang, L., Wei, S., & Zhen, J. (2025). Randomized inspection on listed companies and incremental information disclosure — A study based on MD&A text similarity. *Journal of Accounting and Public Policy*, 54, Article 107382. <https://doi.org/10.1016/j.jaccpubpol.2025.107382>
- Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems*, 36(1), 151–180. <https://doi.org/10.2308/ISYS-2020-067>
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719–749. <https://doi.org/10.1016/j.jfineco.2019.05.019>
- Ke, B., & Zhang, X. (2021). Does public enforcement work in weak investor protection countries? Evidence from China. *Contemporary Accounting Research*, 38(2), 1231–1273. <https://doi.org/10.1111/1911-3846.12652>
- Kesari, A. (2022). Predicting cybersecurity incidents with machine learning and mandatory disclosure regulation. *Illinois Journal of Law, Technology & Policy*, 2022(1), 57–118.
- Kiesow Cortez, E., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, 13(3), 443–463. <https://doi.org/10.1017/err.2022.10>
- Kim, E., & Pae, S. (2025). Voluntary disclosure when information quality is unknown. *The Accounting Review*, 100(2), 269–297. <https://doi.org/10.2308/TAR-2023-0540>
- Kim, Y., & Ryu, D. (2022). Firm-specific or market-wide information: How does analyst coverage influence stock price synchronicity? *Borsa Istanbul Review*, 22(6), 1069–1078. <https://doi.org/10.1016/j.bir.2022.07.011>
- Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications.
- Krueger, P., Sautner, Z., Tang, D. Y., & Zhong, R. (2024). The effects of mandatory ESG disclosure around the world. *Journal of Accounting Research*, 62(5), 1795–1847. <https://doi.org/10.1111/1475-679X.12548>
- Lambert, R., Leuz, C., & Verrecchia, R. E. (2007). Accounting information, disclosure, and the cost of capital. *Journal of Accounting Research*, 45(2), 385–420. <https://doi.org/10.1111/j.1475-679X.2007.00238.x>

- Lang, M. H., Lins, K. V., & Maffett, M. G. (2012). Transparency, liquidity, and valuation: International evidence on when transparency matters most. *Journal of Accounting Research*, 50(3), 729–774. <https://doi.org/10.1111/j.1475-679X.2012.00442.x>
- Lang, M. H., & Lundholm, R. J. (1996). Corporate disclosure policy and analyst behavior. *The Accounting Review*, 71(4), 467–492.
- Lang, M. H., & Stice-Lawrence, L. (2015). Textual analysis and international financial reporting: Large sample evidence. *Journal of Accounting and Economics*, 60(2–3), 110–135. <https://doi.org/10.1016/j.jacceco.2015.09.002>
- La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (2006). What works in securities laws? *The Journal of Finance*, 61(1), 1–32. <https://doi.org/10.1111/j.1540-6261.2006.00828.x>
- La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (2008). The economic consequences of legal origins. *Journal of Economic Literature*, 46(2), 285–332. <https://doi.org/10.1257/jel.46.2.285>
- La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. *Journal of Political Economy*, 106(6), 1113–1155. <https://doi.org/10.1086/250042>
- Leuz, C., Nanda, D., & Wysocki, P. D. (2003). Earnings management and investor protection: An international comparison. *Journal of Financial Economics*, 69(3), 505–527. [https://doi.org/10.1016/S0304-405X\(03\)00121-1](https://doi.org/10.1016/S0304-405X(03)00121-1)
- Leuz, C., & Verrecchia, R. E. (2000). The economic consequences of increased disclosure. *Journal of Accounting Research*, 38, 91–124. <https://doi.org/10.2307/2672910>
- Leuz, C., & Wysocki, P. D. (2016). The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research. *Journal of Accounting Research*, 54(2), 525–622. <https://doi.org/10.1111/1475-679X.12115>
- Li, F. (2008). Annual report readability, current earnings, and earnings persistence. *Journal of Accounting and Economics*, 45(2–3), 221–247. <https://doi.org/10.1016/j.jacceco.2008.02.003>
- Li, F. (2010). The information content of forward-looking statements in corporate filings: A naïve Bayesian machine learning approach. *Journal of Accounting Research*, 48(5), 1049–1102. <https://doi.org/10.1111/j.1475-679X.2010.00382.x>
- Li, H., No, W. G., & Wang, T. (2018). SEC’s cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30,

40–55. <https://doi.org/10.1016/j.accinf.2018.06.003>

Li, L., Zheng, G., & Zhong, A. (2024). Reforming private securities litigation in China: Does private enforcement by minority shareholders matter to corporate fraud? *Finance Research Letters*, 64, Article 105506. <https://doi.org/10.1016/j.frl.2024.105506>

Li, Q., He, L., Gou, X., & Ren, Y. (2024). The registration-based IPO reform and the cost of equity capital: Evidence from China. *Finance Research Letters*, 67, Article 105790. <https://doi.org/10.1016/j.frl.2024.105790>

Lintner, J. (1965). The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets. *The Review of Economics and Statistics*, 47(1), 13–37. <https://doi.org/10.2307/1924119>

Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, 51(1), 62–92. <https://doi.org/10.1177/03128962241293658>

Liu, Z., San, Z., Tsang, A., & Yu, L. (2024). Corporate disclosure differences around the world: International evidence. *Journal of Business Finance & Accounting*, 51(9–10), 2592–2634. <https://doi.org/10.1111/jbfa.12790>

Lo, K., Ramos, F., & Rogo, R. (2017). Earnings management and annual report readability. *Journal of Accounting and Economics*, 63(1), 1–25. <https://doi.org/10.1016/j.jacceco.2016.09.002>

London Stock Exchange Group. (n.d.). *LSEG Workspace* [Database]. Retrieved October 7, 2026, from <https://www.lseg.com/en/data-analytics/products/workspace>

Loughran, T., & McDonald, B. (2011). When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks. *The Journal of Finance*, 66(1), 35–65. <https://doi.org/10.1111/j.1540-6261.2010.01625.x>

Loughran, T., & McDonald, B. (2014). Measuring readability in financial disclosures. *The Journal of Finance*, 69(4), 1643–1671. <https://doi.org/10.1111/jofi.12162>

Loughran, T., & McDonald, B. (2016). Textual analysis in accounting and finance: A survey. *Journal of Accounting Research*, 54(4), 1187–1230. <https://doi.org/10.1111/1475-679X.12123>

Lu, H., Shin, J.-E., & Zhang, M. (2023). Financial reporting and disclosure practices in China. *Journal of Accounting and Economics*, 76(1), Article 101598.

<https://doi.org/10.1016/j.jacceco.2023.101598>

- Mbithi, E., Moloi, T., & Wangombe, D. (2022). Corporate risk disclosure: A systematic literature review and future research agenda. *Cogent Business & Management*, 9(1), Article 2105569. <https://doi.org/10.1080/23311975.2022.2105569>
- Mercer, M. (2004). How do investors assess the credibility of management disclosures? *Accounting Horizons*, 18(3), 185–196. <https://doi.org/10.2308/acch.2004.18.3.185>
- Miihakinen, A. (2012). What drives quality of firm risk disclosure? The impact of a national disclosure standard and reporting incentives under IFRS. *The International Journal of Accounting*, 47(4), 437–468. <https://doi.org/10.1016/j.intacc.2012.10.005>
- Miihakinen, A. (2013). The usefulness of firm risk disclosures under different firm riskiness, investor-interest, and market conditions: New evidence from Finland. *Advances in Accounting*, 29(2), 312–331. <https://doi.org/10.1016/j.adiac.2013.09.006>
- Miller, B. P. (2010). The effects of reporting complexity on small and large investor trading. *The Accounting Review*, 85(6), 2107–2143. <https://doi.org/10.2308/accr.00000001>
- Morse, E. A., Raval, V., & Wingender, J. R., Jr. (2017). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *The Business Lawyer*, 73(1), 1–34.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Neuendorf, K. A. (2017). *The content analysis guidebook* (2nd ed.). SAGE Publications.
- Pástor, L., & Veronesi, P. (2003). Stock valuation and learning about profitability. *The Journal of Finance*, 58(5), 1749–1789. <https://doi.org/10.1111/1540-6261.00587>
- Patel, V., & Michayluk, D. (2016). Return predictability following different drivers of large price changes. *International Review of Financial Analysis*, 45, 202–214. <https://doi.org/10.1016/j.irfa.2016.03.004>
- Reuters. (2017, May 14). *Cyber attack hits 200,000 in at least 150 countries: Europol*. Investing.com. <https://www.investing.com/news/technology-news/cyber-attack-hits-200%2C000-in-at-least-150-countries%3A-europol-484031>
- Richardson, A. J., & Welker, M. (2001). Social disclosure, financial disclosure and the cost of equity

- capital. *Accounting, Organizations and Society*, 26(7–8), 597–616.  
[https://doi.org/10.1016/S0361-3682\(01\)00025-3](https://doi.org/10.1016/S0361-3682(01)00025-3)
- Rjiba, H., Saadi, S., Boubaker, S., & Ding, X. (2021). Annual report readability and the cost of equity capital. *Journal of Corporate Finance*, 67, Article 101902.  
<https://doi.org/10.1016/j.jcorpfin.2021.101902>
- Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, 49, 146–154.  
<https://doi.org/10.1016/j.irfa.2017.01.001>
- Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, 9(1), Article tyad009.  
<https://doi.org/10.1093/cybsec/tyad009>
- Scott, W. R. (2008). *Institutions and organizations: Ideas and interests* (3rd ed.). SAGE Publications.
- Shams, S., Bose, S., Gunasekarage, A., & Velayutham, E. (2024). Does continuous disclosure affect the market reaction to mergers and acquisitions announcements? *Pacific-Basin Finance Journal*, 88, Article 102540. <https://doi.org/10.1016/j.pacfin.2024.102540>
- Sharpe, W. F. (1964). Capital asset prices: A theory of market equilibrium under conditions of risk. *The Journal of Finance*, 19(3), 425–442. <https://doi.org/10.1111/j.1540-6261.1964.tb02865.x>
- Standing Committee of the National People’s Congress. (2016, November 7). *Zhonghua Renmin Gongheguo wangluo anquan fa* [Cybersecurity Law of the People’s Republic of China]. [https://www.cac.gov.cn/2016-11/07/c\\_1119867116.htm](https://www.cac.gov.cn/2016-11/07/c_1119867116.htm)
- Standing Committee of the National People’s Congress. (2021a, June 10). *Zhonghua Renmin Gongheguo shuju anquan fa* [Data Security Law of the People’s Republic of China]. <https://flk.npc.gov.cn/detail?id=ff80818179f5e0800179f885c7e70392>
- Standing Committee of the National People’s Congress. (2021b, August 20). *Zhonghua Renmin Gongheguo geren xinxi baohu fa* [Personal Information Protection Law of the People’s Republic of China]. <https://wb.flk.npc.gov.cn/flfg/PDF/f67af9f12e1b4c83a998cf5a876ce0e4.pdf>
- Sustainability Accounting Standards Board. (2017). *SASB conceptual framework*. <https://sasb.ifrs.org/wp-content/uploads/2019/05/SASB-Conceptual-Framework.pdf>

- Tan, L., Zhang, X., & Zhang, X. (2024). Retail and institutional investor trading behaviors: Evidence from China. *Annual Review of Financial Economics*, 16, 459–483. <https://doi.org/10.1146/annurev-financial-082123-110132>
- Target Corporation. (2014). *2013 annual report*. <https://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm>
- Taylor, S., & Tong, A. (2023). How important are semi-annual earnings announcements? An information event perspective. *Accounting & Finance*, 63(3), 3585–3607. <https://doi.org/10.1111/acfi.13050>
- Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, Article 101795. <https://doi.org/10.1016/j.irfa.2021.101795>
- Tsang, R. C. W., Baldwin, A. A., Hair, J. F., Jr., Affuso, E., & Lahtinen, K. D. (2023). The informativeness of sentiment types in risk factor disclosures: Evidence from firms with cybersecurity breaches. *Journal of Information Systems*, 37(3), 157–190. <https://doi.org/10.2308/ISYS-2022-014>
- U.S. Securities and Exchange Commission. (2011). *CF disclosure guidance: Topic No. 2—Cybersecurity*. <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>
- U.S. Securities and Exchange Commission. (2018). *Commission statement and guidance on public company cybersecurity disclosures* (Release Nos. 33-10459; 34-82746). <https://www.sec.gov/rules/interp/2018/33-10459.pdf>
- U.S. Securities and Exchange Commission. (2023). *Cybersecurity risk management, strategy, governance, and incident disclosure* (Release Nos. 33-11216; 34-97989). <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>
- Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, 5, 179–194. [https://doi.org/10.1016/0165-4101\(83\)90011-3](https://doi.org/10.1016/0165-4101(83)90011-3)
- Verrecchia, R. E. (2001). Essays on disclosure. *Journal of Accounting and Economics*, 32(1–3), 97–180. [https://doi.org/10.1016/S0165-4101\(01\)00025-8](https://doi.org/10.1016/S0165-4101(01)00025-8)
- Wu, H., Ma, M., & Zhang, J. (2025). Impact of cybersecurity disclosure frequency on stock price crash risk. *Journal of Corporate Accounting & Finance*, 36(3), 87–102. <https://doi.org/10.1002/jcaf.22775>

- Yang, M., Li, Y., & Dong, D. (2023). Strategic information disclosure and the cost of equity capital: Evidence from China. *Finance Research Letters*, 51, Article 103418. <https://doi.org/10.1016/j.frl.2022.103418>
- Zhao, Z., Lu, C., & Xia, X. (2024). Regulator as a minority shareholder and corporate fraud: Quasi-natural experiment evidence from the pilot project of China Securities Investor Services Center. *The British Accounting Review*, 56(5), Article 101242. <https://doi.org/10.1016/j.bar.2023.101242>
- Zheng, G., Xia, Z., He, F., & Xiao, Z. (2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk. *Research in International Business and Finance*, 73, Article 102542. <https://doi.org/10.1016/j.ribaf.2024.102542>

## Appendices

### Appendix 3A Sample Construction and Industry Composition

**Table 3A.1**

*Industry Composition of the Original Eligible Pool and Final Locked Sample*

| Country          | Sample stage           | Financials | Technology | Healthcare | Total |
|------------------|------------------------|------------|------------|------------|-------|
| <b>Australia</b> | Original eligible pool | 96         | 39         | 31         | 166   |
| <b>Australia</b> | Final locked sample    | 45         | 28         | 27         | 100   |
| <b>China</b>     | Original eligible pool | 144        | 992        | 483        | 1,619 |
| <b>China</b>     | Final locked sample    | 6          | 65         | 29         | 100   |

*Note.* The original eligible pool refers to the LSEG industry-restricted candidate pool extracted from Financials, Technology, and Healthcare. The final locked sample includes firms retained after annual-report collection and variable-availability screening.

**Table 3A.2***Final Sample Firms by Country and Industry*

| <b>Country</b> | <b>Firm ID</b> | <b>RIC</b> | <b>firm name</b>                 | <b>Industry</b> | <b>Fiscal years included</b> |
|----------------|----------------|------------|----------------------------------|-----------------|------------------------------|
| AU             | AU001          | CGF.AX     | Challenger Ltd                   | Financials      | 2022, 2023, 2024             |
| AU             | AU002          | AYA.AX     | Artrya Ltd                       | Healthcare      | 2022, 2023, 2024             |
| AU             | AU003          | HUM.AX     | Humm Group Ltd                   | Financials      | 2022, 2023, 2024             |
| AU             | AU004          | NGL.AX     | Navigator Global Investments Ltd | Financials      | 2022, 2023, 2024             |
| AU             | AU005          | PXA.AX     | PEXA Group Ltd                   | Technology      | 2022, 2023, 2024             |
| AU             | AU006          | EQT.AX     | EQT Holdings Ltd                 | Financials      | 2022, 2023, 2024             |
| AU             | AU007          | QAL.AX     | Qualitas Ltd                     | Financials      | 2022, 2023, 2024             |
| AU             | AU008          | MPL.AX     | Medibank Private Ltd             | Financials      | 2022, 2023, 2024             |
| AU             | AU009          | TLS.AX     | Telstra Group Ltd                | Technology      | 2022, 2023, 2024             |
| AU             | AU010          | SLC.AX     | Superloop Ltd                    | Technology      | 2022, 2023, 2024             |
| AU             | AU011          | SKS.AX     | SKS Technologies Group Ltd       | Technology      | 2022, 2023, 2024             |
| AU             | AU012          | DXB.AX     | Dimerix Ltd                      | Healthcare      | 2022, 2023, 2024             |
| AU             | AU013          | EIQ.AX     | EchoIQ Ltd                       | Healthcare      | 2022, 2023, 2024             |
| AU             | AU014          | L1G.AX     | L1 Group Ltd                     | Financials      | 2022, 2023, 2024             |
| AU             | AU015          | FID.AX     | Fiducian Group Ltd               | Financials      | 2022, 2023, 2024             |
| AU             | AU016          | DTL.AX     | Data#3 Ltd                       | Technology      | 2022, 2023, 2024             |
| AU             | AU017          | ANN.AX     | Ansell Ltd                       | Healthcare      | 2022, 2023, 2024             |
| AU             | AU018          | CU6.AX     | Clarity Pharmaceuticals Ltd      | Healthcare      | 2022, 2023, 2024             |
| AU             | AU019          | AUB.AX     | AUB Group Ltd                    | Financials      | 2022, 2023, 2024             |

| Country | Firm ID | RIC    | firm name                      | Industry   | Fiscal years included |
|---------|---------|--------|--------------------------------|------------|-----------------------|
| AU      | AU020   | BEN.AX | Bendigo and Adelaide Bank Ltd  | Financials | 2022, 2023, 2024      |
| AU      | AU021   | QOR.AX | Qoria Ltd                      | Technology | 2022, 2023, 2024      |
| AU      | AU022   | MSB.AX | Mesoblast Ltd                  | Healthcare | 2022, 2023, 2024      |
| AU      | AU023   | PPT.AX | Perpetual Ltd                  | Financials | 2022, 2023, 2024      |
| AU      | AU024   | ZIP.AX | Zip Co Ltd                     | Financials | 2022, 2023, 2024      |
| AU      | AU025   | SDF.AX | Steadfast Group Ltd            | Financials | 2022, 2023, 2024      |
| AU      | AU026   | NAN.AX | Nanosonics Ltd                 | Healthcare | 2022, 2023, 2024      |
| AU      | AU027   | OBL.AX | Omni Bridgeway Ltd             | Financials | 2022, 2023, 2024      |
| AU      | AU028   | JDO.AX | Judo Capital Holdings Ltd      | Financials | 2022, 2023, 2024      |
| AU      | AU029   | NXL.AX | Nuix Ltd                       | Technology | 2022, 2023, 2024      |
| AU      | AU030   | XRF.AX | XRF Scientific Ltd             | Technology | 2022, 2023, 2024      |
| AU      | AU031   | OCL.AX | Objective Corporation Ltd      | Technology | 2022, 2023, 2024      |
| AU      | AU032   | HSN.AX | Hansen Technologies Ltd        | Technology | 2022, 2023, 2024      |
| AU      | AU033   | COH.AX | Cochlear Ltd                   | Healthcare | 2022, 2023, 2024      |
| AU      | AU034   | SLX.AX | Silex Systems Ltd              | Technology | 2022, 2023, 2024      |
| AU      | AU035   | SHL.AX | Sonic Healthcare Ltd           | Healthcare | 2022, 2023, 2024      |
| AU      | AU036   | EOL.AX | Energy One Ltd                 | Technology | 2022, 2023, 2024      |
| AU      | AU037   | PNV.AX | Polynovo Ltd                   | Healthcare | 2022, 2023, 2024      |
| AU      | AU038   | CBA.AX | Commonwealth Bank of Australia | Financials | 2022, 2023, 2024      |
| AU      | AU039   | CDA.AX | Codan Ltd                      | Technology | 2022, 2023, 2024      |
| AU      | AU040   | SIG.AX | Sigma Healthcare Ltd           | Healthcare | 2022, 2023,           |

| Country | Firm ID | RIC    | firm name                                | Industry   | Fiscal years included |
|---------|---------|--------|------------------------------------------|------------|-----------------------|
|         |         |        |                                          |            | 2024                  |
| AU      | AU041   | NWL.AX | Netwealth Group Ltd                      | Financials | 2022, 2023, 2024      |
| AU      | AU042   | IMM.AX | Immutep Ltd                              | Healthcare | 2022, 2023, 2024      |
| AU      | AU043   | PME.AX | Pro Medicus Ltd                          | Healthcare | 2022, 2023, 2024      |
| AU      | AU044   | CGS.AX | CogState Ltd                             | Healthcare | 2022, 2023, 2024      |
| AU      | AU045   | PYC.AX | PYC Therapeutics Ltd                     | Healthcare | 2022, 2023, 2024      |
| AU      | AU046   | HUB.AX | Hub24 Ltd                                | Financials | 2022, 2023, 2024      |
| AU      | AU047   | MMS.AX | McMillan Shakespeare Ltd                 | Financials | 2022, 2023, 2024      |
| AU      | AU048   | HLS.AX | Healius Ltd                              | Healthcare | 2022, 2023, 2024      |
| AU      | AU049   | WBT.AX | Weebit Nano Ltd                          | Technology | 2022, 2023, 2024      |
| AU      | AU050   | AFG.AX | Australian Finance Group Ltd             | Financials | 2022, 2023, 2024      |
| AU      | AU051   | NHF.AX | NIB Holdings Ltd                         | Financials | 2022, 2023, 2024      |
| AU      | AU052   | MYS.AX | MyState Ltd                              | Financials | 2022, 2023, 2024      |
| AU      | AU053   | PNL.AX | Pinnacle Investment Management Group Ltd | Financials | 2022, 2023, 2024      |
| AU      | AU054   | ACL.AX | Australian Clinical Labs Ltd             | Healthcare | 2022, 2023, 2024      |
| AU      | AU055   | NXT.AX | NEXTDC Ltd                               | Technology | 2022, 2023, 2024      |
| AU      | AU056   | 4DX.AX | 4DMedical Ltd                            | Healthcare | 2022, 2023, 2024      |
| AU      | AU057   | IFL.AX | Insignia Financial Ltd                   | Financials | 2022, 2023, 2024      |
| AU      | AU058   | CUV.AX | Clinuvel Pharmaceuticals Ltd             | Healthcare | 2022, 2023, 2024      |
| AU      | AU059   | RUL.AX | RPMGlobal Holdings Ltd                   | Technology | 2022, 2023, 2024      |
| AU      | AU060   | MFG.AX | Magellan Financial Group Ltd             | Financials | 2022, 2023, 2024      |

| <b>Country</b> | <b>Firm ID</b> | <b>RIC</b> | <b>firm name</b>               | <b>Industry</b> | <b>Fiscal years included</b> |
|----------------|----------------|------------|--------------------------------|-----------------|------------------------------|
| AU             | AU061          | SVR.AX     | Solvar Ltd                     | Financials      | 2022, 2023, 2024             |
| AU             | AU062          | AD8.AX     | Audinate Group Ltd             | Technology      | 2022, 2023, 2024             |
| AU             | AU063          | MAQ.AX     | Macquarie Technology Group Ltd | Technology      | 2022, 2023, 2024             |
| AU             | AU064          | RHC.AX     | Ramsay Health Care Ltd         | Healthcare      | 2022, 2023, 2024             |
| AU             | AU065          | PGC.AX     | Paragon Care Ltd               | Healthcare      | 2022, 2023, 2024             |
| AU             | AU066          | RAC.AX     | Racura Oncology Ltd            | Healthcare      | 2022, 2023, 2024             |
| AU             | AU067          | MP1.AX     | Megaport Ltd                   | Technology      | 2022, 2023, 2024             |
| AU             | AU068          | SUN.AX     | Suncorp Group Ltd              | Financials      | 2022, 2023, 2024             |
| AU             | AU069          | CNI.AX     | Centuria Capital Group         | Financials      | 2022, 2023, 2024             |
| AU             | AU070          | CAR.AX     | CAR Group Ltd                  | Technology      | 2022, 2023, 2024             |
| AU             | AU071          | WTC.AX     | WiseTech Global Ltd            | Technology      | 2022, 2023, 2024             |
| AU             | AU072          | DRR.AX     | Deterra Royalties Ltd          | Financials      | 2022, 2023, 2024             |
| AU             | AU073          | IAG.AX     | Insurance Australia Group Ltd  | Financials      | 2022, 2023, 2024             |
| AU             | AU074          | REA.AX     | REA Group Ltd                  | Technology      | 2022, 2023, 2024             |
| AU             | AU075          | BVS.AX     | Bravura Solutions Ltd          | Technology      | 2022, 2023, 2024             |
| AU             | AU076          | CVW.AX     | Clearview Wealth Ltd           | Financials      | 2022, 2023, 2024             |
| AU             | AU077          | SDR.AX     | Siteminder Ltd                 | Technology      | 2022, 2023, 2024             |
| AU             | AU078          | ASX.AX     | ASX Ltd                        | Financials      | 2022, 2023, 2024             |
| AU             | AU079          | CCP.AX     | Credit Corp Group Ltd          | Financials      | 2022, 2023, 2024             |
| AU             | AU080          | COG.AX     | COG Financial Services Ltd     | Financials      | 2022, 2023, 2024             |
| AU             | AU081          | LFG.AX     | Liberty Group                  | Financials      | 2022, 2023,                  |

| Country | Firm ID | RIC       | firm name                                     | Industry   | Fiscal years included |
|---------|---------|-----------|-----------------------------------------------|------------|-----------------------|
|         |         |           |                                               |            | 2024                  |
| AU      | AU082   | GDG.AX    | Generation Development Group Ltd              | Financials | 2022, 2023, 2024      |
| AU      | AU083   | PAC.AX    | Pacific Current Group Ltd                     | Financials | 2022, 2023, 2024      |
| AU      | AU084   | AEF.AX    | Australian Ethical Investment Ltd             | Financials | 2022, 2023, 2024      |
| AU      | AU085   | PPS.AX    | Praemium Ltd                                  | Technology | 2022, 2023, 2024      |
| AU      | AU086   | RDY.AX    | Readytech Holdings Ltd                        | Technology | 2022, 2023, 2024      |
| AU      | AU087   | RMC.AX    | Resimac Group Ltd                             | Financials | 2022, 2023, 2024      |
| AU      | AU088   | WRK.AX    | Wrkr Ltd                                      | Technology | 2022, 2023, 2024      |
| AU      | AU089   | HMC.AX    | HMC Capital Ltd                               | Financials | 2022, 2023, 2024      |
| AU      | AU090   | OPT.AX    | Opthea Ltd                                    | Healthcare | 2022, 2023, 2024      |
| AU      | AU091   | IDX.AX    | Integral Diagnostics Ltd                      | Healthcare | 2022, 2023, 2024      |
| AU      | AU092   | CSL.AX    | CSL Ltd                                       | Healthcare | 2022, 2023, 2024      |
| AU      | AU093   | QBE.AX    | QBE Insurance Group Ltd                       | Financials | 2022, 2023, 2024      |
| AU      | AU094   | TPG.AX    | TPG Telecom Ltd                               | Technology | 2022, 2023, 2024      |
| AU      | AU095   | GQG.AX    | GQG Partners Inc                              | Financials | 2022, 2023, 2024      |
| AU      | AU096   | AMP.AX    | AMP Ltd                                       | Financials | 2022, 2023, 2024      |
| AU      | AU097   | BFL.AX    | BSP Financial Group Ltd                       | Financials | 2022, 2023, 2024      |
| AU      | AU098   | TLX.AX    | Telix Pharmaceuticals Ltd                     | Healthcare | 2022, 2023, 2024      |
| AU      | AU099   | NEU.AX    | Neuren Pharmaceuticals Ltd                    | Healthcare | 2022, 2023, 2024      |
| AU      | AU100   | MAF.AX    | MA Financial Group Ltd                        | Financials | 2022, 2023, 2024      |
| CN      | CN001   | 600131.SS | State Grid Information & Communication Co Ltd | Technology | 2022, 2023, 2024      |

| Country | Firm ID | RIC       | firm name                                   | Industry   | Fiscal years included |
|---------|---------|-----------|---------------------------------------------|------------|-----------------------|
| CN      | CN002   | 600589.SS | Dawei Technology Guangdong Group Co Ltd     | Technology | 2022, 2023, 2024      |
| CN      | CN003   | 300555.SZ | Lootom Telcovidio Network Wuxi Co Ltd       | Technology | 2022, 2023, 2024      |
| CN      | CN004   | 603676.SS | Tibet Weixinkang Pharmaceutical Co Ltd      | Healthcare | 2022, 2023, 2024      |
| CN      | CN005   | 300884.SZ | Dnake Xiamen Intelligent Technology Co Ltd  | Technology | 2022, 2023, 2024      |
| CN      | CN006   | 688026.SS | Guangzhou Jet Bio-Filtration Co Ltd         | Healthcare | 2022, 2023, 2024      |
| CN      | CN007   | 300142.SZ | Walvax Biotechnology Co Ltd                 | Healthcare | 2022, 2023, 2024      |
| CN      | CN008   | 688185.SS | CanSino Biologics Inc                       | Healthcare | 2022, 2023, 2024      |
| CN      | CN009   | 301211.SZ | Hubei Biocause Heilen Pharmaceutical Co Ltd | Healthcare | 2022, 2023, 2024      |
| CN      | CN010   | 002189.SZ | Costar Group Co Ltd                         | Technology | 2022, 2023, 2024      |
| CN      | CN011   | 688117.SS | ChengDu Sheng Nuo Biotec Co Ltd             | Healthcare | 2022, 2023, 2024      |
| CN      | CN012   | 002936.SZ | Bank of Zhengzhou Co Ltd                    | Financials | 2022, 2023, 2024      |
| CN      | CN013   | 300684.SZ | Jones Tech PLC                              | Technology | 2022, 2023, 2024      |
| CN      | CN014   | 300513.SZ | Beijing E-techstar Co Ltd                   | Technology | 2022, 2023, 2024      |
| CN      | CN015   | 301065.SZ | Zhejiang Benli Technology Co Ltd            | Healthcare | 2022, 2023, 2024      |
| CN      | CN016   | 300389.SZ | Shenzhen Absen Optoelectronic Co Ltd        | Technology | 2022, 2023, 2024      |
| CN      | CN017   | 688225.SS | Asiainfo Security Technologies Co Ltd       | Technology | 2022, 2023, 2024      |
| CN      | CN018   | 000750.SZ | Sealand Securities Co Ltd                   | Financials | 2022, 2023, 2024      |
| CN      | CN019   | 603042.SS | Nanjing Huamai Technology Co Ltd            | Technology | 2022, 2023, 2024      |
| CN      | CN020   | 601198.SS | Dongxing Securities Corp Ltd                | Financials | 2022, 2023, 2024      |
| CN      | CN021   | 603203.SS | Quick Intelligent Equipment Co Ltd          | Technology | 2022, 2023, 2024      |
| CN      | CN022   | 002851.SZ | Shenzhen Megmeet Electrical Co Ltd          | Technology | 2022, 2023,           |

| Country | Firm ID | RIC       | firm name                                            | Industry   | Fiscal years included |
|---------|---------|-----------|------------------------------------------------------|------------|-----------------------|
|         |         |           |                                                      |            | 2024                  |
| CN      | CN023   | 300300.SZ | Strait Innovation Internet Co Ltd                    | Technology | 2022, 2023, 2024      |
| CN      | CN024   | 688209.SS | Shenzhen Injoinic Technology Co Ltd                  | Technology | 2022, 2023, 2024      |
| CN      | CN025   | 000063.SZ | ZTE Corp                                             | Technology | 2022, 2023, 2024      |
| CN      | CN026   | 300052.SZ | Shenzhen Zqgame Co Ltd                               | Technology | 2022, 2023, 2024      |
| CN      | CN027   | 300942.SZ | Shenzhen Bioeasy Biotechnology Co Ltd                | Healthcare | 2022, 2023, 2024      |
| CN      | CN028   | 300292.SZ | Wutong Holding Group Co Ltd                          | Technology | 2022, 2023, 2024      |
| CN      | CN029   | 603920.SS | Olympic Circuit Technology Co Ltd                    | Technology | 2022, 2023, 2024      |
| CN      | CN030   | 300344.SZ | Cubic Digital Technology Co Ltd                      | Technology | 2022, 2023, 2024      |
| CN      | CN031   | 601009.SS | Bank of Nanjing Co Ltd                               | Financials | 2022, 2023, 2024      |
| CN      | CN032   | 000586.SZ | Sichuan Huiyuan Optical Communications Co Ltd        | Technology | 2022, 2023, 2024      |
| CN      | CN033   | 000636.SZ | Guangdong Fenghua Advanced Technology Holding Co Ltd | Technology | 2022, 2023, 2024      |
| CN      | CN034   | 002446.SZ | Guangdong Shenglu Telecommunication Tech Co Ltd      | Technology | 2022, 2023, 2024      |
| CN      | CN035   | 300396.SZ | Dirui Industrial Co Ltd                              | Healthcare | 2022, 2023, 2024      |
| CN      | CN036   | 300896.SZ | Imeik Technology Development Co Ltd                  | Healthcare | 2022, 2023, 2024      |
| CN      | CN037   | 301166.SZ | Shanghai Universal Biotech Co Ltd                    | Healthcare | 2022, 2023, 2024      |
| CN      | CN038   | 688027.SS | Quantum CTEK Co Ltd                                  | Technology | 2022, 2023, 2024      |
| CN      | CN039   | 002907.SZ | Chongqing Pharscin Pharmaceutical Co Ltd             | Healthcare | 2022, 2023, 2024      |
| CN      | CN040   | 688232.SS | Guotai Epont Software Co Ltd                         | Technology | 2022, 2023, 2024      |
| CN      | CN041   | 605588.SS | Keystone Technology Co Ltd                           | Technology | 2022, 2023, 2024      |
| CN      | CN042   | 603712.SS | TianJin 712 Communication & Broadcasting Co Ltd      | Technology | 2022, 2023, 2024      |

| Country | Firm ID | RIC       | firm name                                                  | Industry   | Fiscal years included |
|---------|---------|-----------|------------------------------------------------------------|------------|-----------------------|
| CN      | CN043   | 300238.SZ | Guanhao Biotech Co Ltd                                     | Healthcare | 2022, 2023, 2024      |
| CN      | CN044   | 002872.SZ | Tiansheng Pharmaceutical Group Co Ltd                      | Healthcare | 2022, 2023, 2024      |
| CN      | CN045   | 301180.SZ | Suzhou Wanxiang Technology Co Ltd                          | Technology | 2022, 2023, 2024      |
| CN      | CN046   | 300418.SZ | Kunlun Tech Co Ltd                                         | Technology | 2022, 2023, 2024      |
| CN      | CN047   | 688012.SS | Advanced Micro-Fabrication Equipment Inc China             | Technology | 2022, 2023, 2024      |
| CN      | CN048   | 002322.SZ | Ningbo Ligong Environment and Energy Technology Co Ltd     | Technology | 2022, 2023, 2024      |
| CN      | CN049   | 688127.SS | Zhejiang Lante Optics Co Ltd                               | Technology | 2022, 2023, 2024      |
| CN      | CN050   | 002138.SZ | Shenzhen Sunlord Electronics Co Ltd                        | Technology | 2022, 2023, 2024      |
| CN      | CN051   | 688338.SS | Beijing Succeeder Technology Inc                           | Healthcare | 2022, 2023, 2024      |
| CN      | CN052   | 002030.SZ | Daan Gene Co Ltd                                           | Healthcare | 2022, 2023, 2024      |
| CN      | CN053   | 605186.SS | Shanghai General Healthy Information and Technology Co Ltd | Healthcare | 2022, 2023, 2024      |
| CN      | CN054   | 002675.SZ | Yantai Dongcheng Biochemicals Co Ltd                       | Healthcare | 2022, 2023, 2024      |
| CN      | CN055   | 688016.SS | Shanghai MicroPort Endovascular MedTech Group Co Ltd       | Healthcare | 2022, 2023, 2024      |
| CN      | CN056   | 301221.SZ | Wuhan Kotei Informatics Co Ltd                             | Technology | 2022, 2023, 2024      |
| CN      | CN057   | 688030.SS | Hillstone Networks Co Ltd                                  | Technology | 2022, 2023, 2024      |
| CN      | CN058   | 002289.SZ | Shenzhen Success Electronics Co Ltd                        | Technology | 2022, 2023, 2024      |
| CN      | CN059   | 301111.SZ | Guangdong Lifestrong Pharmacy Co Ltd                       | Healthcare | 2022, 2023, 2024      |
| CN      | CN060   | 002742.SZ | Chongqing Sansheng Industrial Co Ltd                       | Healthcare | 2022, 2023, 2024      |
| CN      | CN061   | 600071.SS | Phenix Optics Co Ltd                                       | Technology | 2022, 2023, 2024      |
| CN      | CN062   | 002402.SZ | Shenzhen H&T Intelligent Control Co Ltd                    | Technology | 2022, 2023, 2024      |
| CN      | CN063   | 603566.SS | Pulike Biological Engineering Inc                          | Healthcare | 2022, 2023,           |

| Country | Firm ID | RIC       | firm name                                                        | Industry   | Fiscal years included |
|---------|---------|-----------|------------------------------------------------------------------|------------|-----------------------|
|         |         |           |                                                                  |            | 2024                  |
| CN      | CN064   | 603738.SS | TKD Science and Technology Co Ltd                                | Technology | 2022, 2023, 2024      |
| CN      | CN065   | 002197.SZ | SZZT Electronics Co Ltd                                          | Technology | 2022, 2023, 2024      |
| CN      | CN066   | 002952.SZ | Yes Optoelectronics Group Co Ltd                                 | Technology | 2022, 2023, 2024      |
| CN      | CN067   | 603087.SS | Gan & Lee Pharmaceuticals                                        | Healthcare | 2022, 2023, 2024      |
| CN      | CN068   | 300098.SZ | Gosuncn Technology Group Co Ltd                                  | Technology | 2022, 2023, 2024      |
| CN      | CN069   | 601077.SS | Chongqing Rural Commercial Bank Co Ltd                           | Financials | 2022, 2023, 2024      |
| CN      | CN070   | 002199.SZ | Zhejiang East Crystal Electronic Co Ltd                          | Technology | 2022, 2023, 2024      |
| CN      | CN071   | 600498.SS | Fiberhome Telecommunication Technologies Co Ltd                  | Technology | 2022, 2023, 2024      |
| CN      | CN072   | 600130.SS | Ningbo Bird Co Ltd                                               | Technology | 2022, 2023, 2024      |
| CN      | CN073   | 688175.SS | Zhuhai Comleader Information Science & Technology Co Ltd         | Technology | 2022, 2023, 2024      |
| CN      | CN074   | 300359.SZ | Qtone Education Group Guangdong Co Ltd                           | Technology | 2022, 2023, 2024      |
| CN      | CN075   | 300991.SZ | Shenzhen Chuangyitong Technology Co Ltd                          | Technology | 2022, 2023, 2024      |
| CN      | CN076   | 002512.SZ | Tatwah Smartech Co Ltd                                           | Technology | 2022, 2023, 2024      |
| CN      | CN077   | 688618.SS | 3onedata Co Ltd                                                  | Technology | 2022, 2023, 2024      |
| CN      | CN078   | 603703.SS | Zhejiang Shengyang Science and Technology Co Ltd                 | Technology | 2022, 2023, 2024      |
| CN      | CN079   | 600998.SS | Jointown Pharmaceutical Group Co Ltd                             | Healthcare | 2022, 2023, 2024      |
| CN      | CN080   | 300177.SZ | Guangzhou Hi Target Navigation Tech Co Ltd                       | Technology | 2022, 2023, 2024      |
| CN      | CN081   | 600764.SS | China Marine Information Electronics Co Ltd                      | Technology | 2022, 2023, 2024      |
| CN      | CN082   | 301130.SZ | Jilin Province Xidian Pharmaceutical Sci-Tech Development Co Ltd | Healthcare | 2022, 2023, 2024      |
| CN      | CN083   | 300183.SZ | Qingdao Eastsoft Communication Technology Co Ltd                 | Technology | 2022, 2023, 2024      |

| Country | Firm ID | RIC       | firm name                                          | Industry   | Fiscal years included |
|---------|---------|-----------|----------------------------------------------------|------------|-----------------------|
| CN      | CN084   | 300768.SZ | Hangzhou DPtech Technologies Co Ltd                | Technology | 2022, 2023, 2024      |
| CN      | CN085   | 603501.SS | OmniVision Integrated Circuits Group Inc           | Technology | 2022, 2023, 2024      |
| CN      | CN086   | 000889.SZ | ZJBC Information Technology Co Ltd                 | Technology | 2022, 2023, 2024      |
| CN      | CN087   | 300937.SZ | SICHUAN HZ-YEG MEDICAL Co Ltd                      | Healthcare | 2022, 2023, 2024      |
| CN      | CN088   | 002879.SZ | Chang Lan Technology Group Co Ltd                  | Technology | 2022, 2023, 2024      |
| CN      | CN089   | 300075.SZ | Beijing eGOVA Co Ltd                               | Technology | 2022, 2023, 2024      |
| CN      | CN090   | 688278.SS | Xiamen Amoytop Biotech Co Ltd                      | Healthcare | 2022, 2023, 2024      |
| CN      | CN091   | 603718.SS | Shanghai Hile Bio-Technology Co Ltd                | Healthcare | 2022, 2023, 2024      |
| CN      | CN092   | 300036.SZ | Beijing SuperMap Software Co Ltd                   | Technology | 2022, 2023, 2024      |
| CN      | CN093   | 688181.SS | Beijing Bayi Space LCD Technology Co Ltd           | Technology | 2022, 2023, 2024      |
| CN      | CN094   | 002421.SZ | Shenzhen Das Intellitech Co Ltd                    | Technology | 2022, 2023, 2024      |
| CN      | CN095   | 002119.SZ | Ningbo Kangqiang Electronics Co Ltd                | Technology | 2022, 2023, 2024      |
| CN      | CN096   | 603222.SS | Chimin Health Management Co Ltd                    | Healthcare | 2022, 2023, 2024      |
| CN      | CN097   | 300288.SZ | Guiyang Longmaster Information & Technology Co Ltd | Technology | 2022, 2023, 2024      |
| CN      | CN098   | 688228.SS | Ucap Cloud Information Technology Co Ltd           | Technology | 2022, 2023, 2024      |
| CN      | CN099   | 601788.SS | Everbright Securities Co Ltd                       | Financials | 2022, 2023, 2024      |
| CN      | CN100   | 002231.SZ | Allwin Telecommunication Co Ltd                    | Technology | 2022, 2023, 2024      |

*Note.* The table lists the 200 final sample firms after firm-level deduplication. Each retained firm contributes observations for FY2022, FY2023, and FY2024.

## Appendix 3B. CSRDS Measurement Instrument

**Table 3B.1**

### *CSRDS Indicators and Definitions*

| Dimension   | Code | Indicator                              | Definition and coding focus                                                                                                                                                                                                             | Typical report sections                                                                                                |
|-------------|------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Specificity | S1   | Specific cyber threats                 | Identifies concrete cyber threat families or attack vectors rather than generic references to cyber attacks.                                                                                                                            | Risk factors; cybersecurity or IT risk; management discussion; governance risk                                         |
| Specificity | S2   | Cyber resilience and readiness         | Describes testing, drills, monitoring, or response arrangements through specific mechanisms, frequency, or measurable targets, such as penetration testing, red team exercises, recovery time objectives, or recovery point objectives. | Risk management; business continuity; cyber resilience; IT or security operations; management discussion               |
| Specificity | S3   | Cyber risks to key assets              | Links cyber risk to named core assets, systems, or data and explains why they are critical to operations or firm value.                                                                                                                 | Risk factors; IT architecture; governance and operations; digital transformation or fintech sections                   |
| Relevance   | R1   | Active cyber governance                | Demonstrates active governance through the frequency of board oversight, cyber expertise, accountability, or links to executive incentives.                                                                                             | Corporate governance; risk oversight; board committee reports                                                          |
| Relevance   | R2   | Cyber risk and business consequences   | Explains how cyber risk may lead to operational or financial consequences through specific business processes or value chain links, rather than merely stating that operations may be disrupted.                                        | Management discussion; operating and financial review; risk factors; business continuity or disaster recovery sections |
| Relevance   | R3   | Third party and compliance cyber risks | Describes third party or supply chain cyber risk management and specific compliance, certification, or regulatory exposures.                                                                                                            | Governance; risk management; supplier or outsourcing sections; compliance sections                                     |
| Usefulness  | U1   | Quantified cybersecurity resources     | Quantifies cybersecurity resources, such as expenditure, headcount, training hours, or other interpretable resource measures.                                                                                                           | Management discussion; ESG or sustainability reporting; digital transformation; notes to accounts                      |
| Usefulness  | U2   | Cyber insurance and exposure           | Discloses cyber insurance arrangements or quantified exposure boundaries, such as coverage limits, deductibles, or maximum probable loss.                                                                                               | Risk factors; insurance notes; governance; risk management                                                             |

| <b>Dimension</b> | <b>Code</b> | <b>Indicator</b>                  | <b>Definition and coding focus</b>                                                                                                                                   | <b>Typical report sections</b>                                                                           |
|------------------|-------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Usefulness       | U3          | Cybersecurity performance metrics | Provides measurable cybersecurity performance or assurance outcomes, such as response time, patching rates, blocked attacks, system availability, or audit findings. | IT or security operations; ESG reporting; governance; risk management; operations or technology sections |

*Note.* The indicator names are aligned with the terminology used in the main CSRDS codebook and the empirical analyses. The listed report sections identify common locations for evidence and do not restrict coding to those sections.

**Table 3B.2***CSRDS Scoring Criteria*

| <b>Code</b> | <b>Scale</b> | <b>Score 0</b>                                               | <b>Score 1</b>                                                                                           | <b>Score 2</b>                                                                                                               | <b>Evidence requirements</b>                                                                            |
|-------------|--------------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| S1          | 0–2          | No concrete threat named.                                    | Generic labels only (e.g., hacking, virus, cyber attack).                                                | At least one identifiable threat family/vector (e.g., ransomware, phishing, DDoS, supply-chain injection, APT, RDP exploit). | Quote or paraphrase must include the named threat; record page/section.                                 |
| S2          | 0–2          | No mention of testing/drills/monitoring /response mechanism. | Mentions existence of plans/monitoring generically (e.g., ‘we have an incident response plan’).          | Specific details: frequency, third-party testing, outcomes, tabletop/red-blue exercises, RTO/RPO, SOC 24/7 with metrics.     | Evidence must include at least one of: frequency, independent test, measurable target, or test outcome. |
| S3          | 0–2          | Boilerplate (systems may be attacked) with no asset context. | Broad assets only (e.g., ‘customer data’, ‘online services’) without specific core asset identification. | Named core assets (e.g., core payment system, trading algorithm, biometric database, CII) + rationale/criticality.           | Record the asset name(s) and the stated rationale (critical operations/value-chain relevance).          |
| R1          | 0–2          | No governance disclosure.                                    | Static structure only (e.g., ‘audit committee oversees cyber risk’).                                     | Specific dynamic signals (e.g., quarterly CISO reporting, board cyber expert, KPI in remuneration).                          | Must cite the action/cadence/expertise/accountability language, not just committee names.               |

| Code | Scale | Score 0                                                                                                                                | Score 1                                                                                                                 | Score 2                                                                                                                            | Evidence requirements                                                                                                                                                                                                      |
|------|-------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R2   | 0–2   | No identifiable operational, financial, regulatory, customer, reputational, or continuity consequence is linked to cybersecurity risk. | An identifiable business consequence is stated, but no specific business process or transmission mechanism is explained | A specific business process or value-chain link is identified together with concrete consequence or transmission logic.            | For Score 1, the consequence must be explicitly linked to cybersecurity risk. For Score 2, the evidence should additionally identify a specific business process or value-chain link and the associated consequence logic. |
| R3   | 0–2   | No mention of third-party/compliance signals.                                                                                          | Generic ‘we comply with laws/standards’ with no detail.                                                                 | Specific supplier assurance (audits, requirements) and/or certifications (ISO 27001, MLPS level) with clear level/scope/frequency. | Record the specific standard/certification level or supplier control mechanism.                                                                                                                                            |
| U1   | 0–2   | Qualitative only (e.g., ‘increase investment’).                                                                                        | Vague quantification (percent change only) without base/amount.                                                         | Concrete figures (currency amounts, headcount, training volume) and timeframe.                                                     | Capture unit, amount, and whether explicitly cybersecurity vs general IT/digital spend.                                                                                                                                    |
| U2   | 0–2   | No insurance/exposure disclosure.                                                                                                      | Mentions having cyber insurance without details.                                                                        | Discloses limits/deductibles/coverage scope or quantified exposure/MPL estimate.                                                   | Record numeric coverage info or exposure bound; note if disclosed elsewhere (risk note).                                                                                                                                   |
| U3   | 0–2   | No metrics or outcomes.                                                                                                                | Generic outcomes (e.g., ‘operations stable’).                                                                           | Specific KPIs with numbers/targets and timeframe; or specific assurance outcomes.                                                  | Must include at least one numeric KPI or explicit assurance outcome tied to security.                                                                                                                                      |

**Table 3B.3***Active Bilingual Keyword Dictionary by Indicator*

| <b>Indicator</b> | <b>Active English keywords</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>Active Chinese keywords</b>                                                                                                                                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S1               | ransomware; phishing; DDoS; credential stuffing; zero-day; RDP; advanced persistent threat; supply chain attack; supply chain compromise; software supply chain; business email compromise; insider threat                                                                                                                                                                                                                                                                       | 勒索; 钓鱼; DDoS; 撞库; 零日; RDP; 供应链攻击; 软件供应链安全; 内部威胁                                                                                                                |
| S2               | penetration test; red team; tabletop; disaster recovery; simulation; incident response exercise; recovery point objective; recovery time objective; security operations center                                                                                                                                                                                                                                                                                                   | 渗透测试; 红蓝对抗; 桌面推演; 灾备演练; 7×24 监控; 护网行动; 容灾; 系统容灾; 灾难恢复; 备份恢复; 网络安全应急预案; 信息安全应急响应; 网络安全演练                                                                        |
| S3               | core system; payment platform; trading system; PII; biometric; CII; trade secret; source code; customer data; personal data; sensitive data; financial data; health data; medical records; critical infrastructure; data asset; IT infrastructure; information infrastructure; proprietary data; proprietary system; intellectual property theft                                                                                                                                 | 核心系统; 支付平台; 交易系统; 个人信息; 生物识别; 关基; 商业秘密; 源代码; 核心算法; 客户数据; 个人数据; 敏感数据; 金融数据; 医疗数据; 数据资产; 关键基础设施; 知识产权数据                                                          |
| R1               | board oversight; cyber expertise; CISO reporting; remuneration KPI; audit committee; risk committee; cyber committee; CISO; chief information security officer; chief security officer; CSO; security governance; cyber governance; board review; board briefing; board responsibility; management oversight; executive oversight; security officer; information security officer; cyber risk committee; information security committee; technology committee; digital committee | 董事会监督; CISO 汇报; 薪酬考核 KPI; 一把手负责制; 网络安全专业; 信息安全专业; CISSP; CISM; 风险委员会; 信息安全委员会; 网络安全委员会; 技术委员会; 信息安全管理委员会; 首席信息安全官; 信息安全负责人; 网络安全负责人; 安全治理; 网络安全治理; 管理层监督; 领导小组 |
| R2               | business continuity; operational disruption; outage; penalty; service disruption; system failure; data loss; financial loss; reputational damage; regulatory action; system outage; notifiable data breach; regulatory penalty; regulatory fine                                                                                                                                                                                                                                  | 业务连续性; 中断; 停机; 监管处罚; 牌照风险; 服务中断; 系统故障; 数据丢失; 经济损失; 声誉损失; 监管风险; 监管罚款                                                                                            |
| R3               | ISO 27001; third-party audit; vendor management; APRA CPS 234; CPS 234; Essential Eight; SOC 2;                                                                                                                                                                                                                                                                                                                                                                                  | ISO27001; 第三方审计; 供应商管理; 等保三级; 数据安全法; 个人信息保护法; 网络安全法; IT 外包;                                                                                                    |

| Indicator | Active English keywords                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Active Chinese keywords                                                                                                                           |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|           | NIST; IT outsourcing; technology outsourcing;<br>Privacy Act 1988; SOCI Act                                                                                                                                                                                                                                                                                                                                                                                                              | 信息化外包                                                                                                                                             |
| U1        | security budget; cyber spend; training hours; cyber investment; security investment; IT security budget; cyber budget; information security budget; security spend; security personnel; security staff; security employees; cyber training; security training; awareness training; security awareness; invested in cyber; invested in security; security resources; dedicated security; security headcount; security team size                                                           | 安全预算; 网络安全投入; 专职人员; 培训人次/小时; 投入占比; 网络安全费用; 信息安全费用; 安全建设投入; 安全人员; 安全团队; 专职安全; 安全培训; 网络安全培训; 信息安全培训; 培训课时; 培训次数; 培训人员; 安全意识; 网络安全意识; 网络安全预算; 信息安全经费 |
| U2        | cyber insurance; coverage limit; maximum possible loss; policy limit; limit of indemnity; cyber liability insurance; cyber insurance deductible                                                                                                                                                                                                                                                                                                                                          | 网络安全保险; 保险额度; 免赔额; 最大可能损失; 网络安全敞口; 网络风险敞口; 网络责任保险; 网络风险保险; 网络保险                                                                                   |
| U3        | MTTR; patching rate; blocked attacks; uptime; assurance outcomes; vulnerability remediation; patch management; mean time to; security kpi; security metric; security target; no material incident; no significant incident; zero material; service availability; system availability; security audit result; no breach; no material breach; no data breach; security performance; security outcome; security measure; security audit finding; cyber audit result; no reportable incident | MTTR; 漏洞修复率; 阻断次数; 可用性; 审计结论; 零重大事故; 漏洞整改; 补丁管理; 安全指标; 安全绩效; 安全目标; 安全考核; 无重大事故; 未发生重大; 安全事件处置; 系统可用性; 漏洞数量; 安全运营; 运营指标; 信息安全审计结论; 网络安全审计结果        |

*Note.* Keywords are reported from the final keyword dictionary used in the analysis. They are used as evidence-extraction aids rather than as standalone scoring criteria.

### Appendix 3C. CSRDS Scoring Validation and Reliability

**Table 3C.1**

*Indicator-Level Machine–Human Reliability for CSRDS Scoring*

| Indicator                                 | N   | Disagreements | Agreement % | Agreement 95% CI | Unweighted $\kappa$ | Linear-weighted $\kappa$ | Quadratic-weighted $\kappa$ |
|-------------------------------------------|-----|---------------|-------------|------------------|---------------------|--------------------------|-----------------------------|
| S1 Specific cyber threats                 | 36  | 0             | 100.00      | [90.36, 100.00]  | 1.000               | 1.000                    | 1.000                       |
| S2 Cyber resilience and readiness         | 36  | 2             | 94.44       | [81.86, 98.46]   | 0.915               | 0.935                    | 0.955                       |
| S3 Cyber risks to key assets              | 36  | 0             | 100.00      | [90.36, 100.00]  | 1.000               | 1.000                    | 1.000                       |
| R1 Active cyber governance                | 36  | 2             | 94.44       | [81.86, 98.46]   | 0.829               | 0.849                    | 0.879                       |
| R2 Cyber risk and business consequences   | 36  | 0             | 100.00      | [90.36, 100.00]  | 1.000               | 1.000                    | 1.000                       |
| R3 Third-party and compliance cyber risks | 36  | 0             | 100.00      | [90.36, 100.00]  | 1.000               | 1.000                    | 1.000                       |
| U1 Quantified cybersecurity resources     | 36  | 0             | 100.00      | [90.36, 100.00]  | 1.000               | 1.000                    | 1.000                       |
| U2 Cyber insurance and exposure           | 36  | 0             | 100.00      | [90.36, 100.00]  | 1.000               | 1.000                    | 1.000                       |
| U3 Cybersecurity performance metrics      | 36  | 1             | 97.22       | [85.83, 99.51]   | 0.929               | 0.939                    | 0.952                       |
| Overall                                   | 324 | 5             | 98.46       | [96.44, 99.34]   | 0.969               | 0.975                    | 0.982                       |

*Note.* The validation sample consists of 36 firm-year observations and 324 paired indicator-level decisions. Agreement 95% confidence intervals are Wilson intervals. The overall row is based on 319 agreements and five documented corrections. Unweighted, linear-weighted, and quadratic-weighted kappa are calculated using the final validation definitions. Bootstrap kappa confidence intervals for the full, Australian, and Chinese samples are reported in Table 3C.2.

**Table 3C.2***Country-Specific Validation Reliability and Confidence Intervals**Panel A. Agreement and firm-year exact match*

| Sample      | Firm-year N | Indicator decisions | Disagreements | Agreement % | Agreement 95% CI | Exact-match N | Exact-match % | Exact-match 95% CI |
|-------------|-------------|---------------------|---------------|-------------|------------------|---------------|---------------|--------------------|
| Full sample | 36          | 324                 | 5             | 98.46       | [96.44, 99.34]   | 32            | 88.89         | [74.69, 95.59]     |
| Australia   | 18          | 162                 | 4             | 97.53       | [93.82, 99.04]   | 15            | 83.33         | [60.78, 94.16]     |
| China       | 18          | 162                 | 1             | 99.38       | [96.59, 99.89]   | 17            | 94.44         | [74.24, 99.01]     |

*Panel B. Cohen's kappa estimates and 95% confidence intervals*

| Sample      | Unweighted $\kappa$ | 95% CI           | Linear-weighted $\kappa$ | 95% CI           | Quadratic-weighted $\kappa$ | 95% CI           |
|-------------|---------------------|------------------|--------------------------|------------------|-----------------------------|------------------|
| Full sample | 0.9690              | [0.9372, 0.9940] | 0.9754                   | [0.9501, 0.9951] | 0.9825                      | [0.9648, 0.9965] |
| Australia   | 0.9507              | [0.9009, 1.0000] | 0.9624                   | [0.9250, 1.0000] | 0.9744                      | [0.9482, 1.0000] |
| China       | 0.9875              | [0.9534, 1.0000] | 0.9896                   | [0.9613, 1.0000] | 0.9923                      | [0.9721, 1.0000] |

*Note.* Agreement and firm-year exact-match confidence intervals are Wilson 95% intervals. Kappa confidence intervals are percentile 95% intervals from 10,000 valid firm-year bootstrap replications for each coefficient and sample. The bootstrap resamples firm-year rows so that the nine indicator decisions within each selected observation remain clustered. The manual validation scores reflect the five documented codebook re-judgement corrections applied before the final dataset was locked.

**Table 3C.3***Documented Indicator-Level Corrections in the Post-Refinement Validation*

| <b>Firm-year</b> | <b>Country</b> | <b>FY</b> | <b>Indicator</b> | <b>Machine score</b> | <b>Manual re-judgement</b> | <b>Change</b> |
|------------------|----------------|-----------|------------------|----------------------|----------------------------|---------------|
| AU023/2023       | AU             | 2023      | R1               | 2                    | 1                          | -1            |
| AU029/2022       | AU             | 2022      | R1               | 2                    | 1                          | -1            |
| AU029/2022       | AU             | 2022      | U3               | 2                    | 1                          | -1            |
| AU079/2024       | AU             | 2024      | S2               | 2                    | 1                          | -1            |
| CN067/2022       | CN             | 2022      | S2               | 2                    | 1                          | -1            |

*Note.* These are the five indicator-level disagreements identified during the post-refinement validation.

## Appendix 3D Regression Variable Definitions and Measurement

**Table 3D.1**

### *Definitions and Measurement of Regression Variables*

| <b>Variable</b>     | <b>Definition and measurement</b>                                                                        | <b>Data source</b>                  |
|---------------------|----------------------------------------------------------------------------------------------------------|-------------------------------------|
| CoE                 | Cost of equity measured using the method described in Section 3.4.2                                      | LSEG and country year market inputs |
| CSRDS               | Sum of the nine CSRDS indicators, ranging from 0 to 18                                                   | Annual reports and CSRDS coding     |
| Specificity         | Sum of S1, S2, and S3, ranging from 0 to 6                                                               | Annual reports and CSRDS coding     |
| Relevance           | Sum of R1, R2, and R3, ranging from 0 to 6                                                               | Annual reports and CSRDS coding     |
| Usefulness          | Sum of U1, U2, and U3, ranging from 0 to 6                                                               | Annual reports and CSRDS coding     |
| Australia           | Indicator equal to one for Australian firm-year observations and zero for Chinese firm-year observations | Sample classification               |
| Firm size           | Natural logarithm of total assets                                                                        | LSEG                                |
| Leverage            | Total liabilities divided by total assets                                                                | LSEG                                |
| ROA                 | Net income divided by total assets                                                                       | LSEG                                |
| Earnings volatility | Standard deviation of ROA over the available observation period                                          | Constructed from LSEG data          |
| Analyst coverage    | Natural logarithm of one plus the number of analysts                                                     | LSEG                                |
| Loss dummy          | Indicator equal to one when net income is negative and zero otherwise                                    | LSEG                                |
| Liquidity           | Natural logarithm of average daily trading volume                                                        | LSEG                                |
| Book to market      | Book value of equity divided by market value of equity                                                   | LSEG                                |
| Listing age         | Natural logarithm of one plus the number of years since listing                                          | LSEG                                |

## Appendix 4A. Supplementary H2 Evidence

**Table 4A.1**

### *CAPM R2-Only Model*

| Variable                                  | R2 only               |
|-------------------------------------------|-----------------------|
| S1 Specific cyber threats                 |                       |
| S2 Cyber resilience and readiness         |                       |
| S3 Cyber risks to key assets              |                       |
| R1 Active cyber governance                |                       |
| R2 Cyber risk and business consequences   | -0.0121***<br>(-2.83) |
| R3 Third-party and compliance cyber risks |                       |
| U1 Quantified cybersecurity resources     |                       |
| U2 Cyber insurance and exposure           |                       |
| U3 Cybersecurity performance metrics      |                       |
| Australia                                 | 0.0345***<br>(4.23)   |
| Firm size                                 | -0.0059***<br>(-3.82) |
| Leverage                                  | -0.0049<br>(-0.89)    |
| ROA                                       | -0.0074<br>(-0.77)    |
| Earnings volatility                       | -0.0033<br>(-0.14)    |
| Analyst coverage                          | 0.0024<br>(1.12)      |
| Loss dummy                                | 0.0017<br>(0.41)      |
| Liquidity                                 | 0.0083***<br>(3.65)   |
| Book-to-market                            | 0.0095<br>(1.62)      |
| Listing age                               | -0.0046**<br>(-2.06)  |
| FY2023                                    | 0.0201***<br>(12.73)  |
| FY2024                                    | 0.0050***<br>(4.08)   |
| Year fixed effects                        | Yes                   |
| Firm-clustered SE                         | Yes                   |
| N                                         | 600                   |
| Adjusted R <sup>2</sup>                   | 0.266                 |

*Note.* The dependent variable is the CAPM based cost of equity. The model includes the Australia indicator, the full set of firm level controls, and fiscal year fixed effects. Standard errors are clustered by firm, and t statistics are reported in parentheses. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

**Table 4A.2***H2 Single-Indicator Screening Regressions*

| Indicator                                 | CAPM<br>coefficient<br>(t-statistic) | CAPM<br>p | CAPM<br>Adj. R <sup>2</sup> | LSEG WACC<br>coefficient<br>(t-statistic) | LSEG<br>p | LSEG<br>Adj. R <sup>2</sup> |
|-------------------------------------------|--------------------------------------|-----------|-----------------------------|-------------------------------------------|-----------|-----------------------------|
| S1 Specific cyber threats                 | 0.0019<br>(0.67)                     | .503      | 0.246                       | 0.0005<br>(0.23)                          | .822      | 0.131                       |
| S2 Cyber resilience and readiness         | -0.0009<br>(-0.35)                   | .724      | 0.245                       | -0.0007<br>(-0.32)                        | .748      | 0.131                       |
| S3 Cyber risks to key assets              | 0.0035<br>(0.97)                     | .333      | 0.248                       | 0.0006<br>(0.21)                          | .834      | 0.131                       |
| R1 Active cyber governance                | 0.0063<br>(1.15)                     | .251      | 0.248                       | -0.0054*<br>(-1.80)                       | .072      | 0.134                       |
| R2 Cyber risk and business consequences   | -0.0121***<br>(-2.83)                | .005      | 0.266                       | -0.0079**<br>(-2.18)                      | .030      | 0.143                       |
| R3 Third-party and compliance cyber risks | 0.0015<br>(0.50)                     | .616      | 0.245                       | -0.0014<br>(-0.43)                        | .669      | 0.131                       |
| U1 Quantified cybersecurity resources     | 0.0004<br>(0.08)                     | .933      | 0.245                       | -0.0032<br>(-1.04)                        | .300      | 0.131                       |
| U2 Cyber insurance and exposure           | 0.0095<br>(0.70)                     | .481      | 0.248                       | 0.0103<br>(1.07)                          | .286      | 0.135                       |
| U3 Cybersecurity performance metrics      | 0.0072<br>(1.04)                     | .297      | 0.249                       | -0.0053<br>(-0.97)                        | .334      | 0.134                       |

*Note.* Each row reports a separate regression in which one CSRDS indicator is entered with the full set of firm-level controls and fiscal-year fixed effects. Standard errors are clustered by firm. The CAPM columns use the CAPM based cost of equity as the dependent variable, while the LSEG columns use LSEG StarMine WACC. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

## Appendix 4B. Supplementary H3 Evidence

**Table 4B.1**

*CAPM Country-Subsample Regression Results for H3 Supplementary Analysis*

| Variable                                   | (1) AU: CSRDS<br>score | (2) AU: R2            | (3) CN: CSRDS<br>score | (4) CN: R2           |
|--------------------------------------------|------------------------|-----------------------|------------------------|----------------------|
| Intercept                                  | 0.1198***<br>(3.72)    | 0.1128***<br>(3.46)   | -0.0419<br>(-1.07)     | -0.0394<br>(-0.99)   |
| CSRDS score                                | -0.0004<br>(-0.24)     |                       | 0.0017*<br>(1.90)      |                      |
| R2 Cyber risk and business<br>consequences |                        | -0.0121**<br>(-2.46)  |                        | 0.0021<br>(0.32)     |
| Firm size                                  | -0.0064***<br>(-3.80)  | -0.0066***<br>(-4.01) | -0.0019<br>(-1.01)     | -0.0015<br>(-0.76)   |
| Leverage                                   | -0.0021<br>(-0.26)     | -0.0015<br>(-0.19)    | -0.0199**<br>(-2.26)   | -0.0173*<br>(-1.95)  |
| ROA                                        | -0.0118<br>(-1.30)     | -0.0120<br>(-1.33)    | 0.0215<br>(1.64)       | 0.0235*<br>(1.74)    |
| Earnings volatility                        | 0.0027<br>(0.08)       | -0.0041<br>(-0.13)    | 0.0148<br>(0.48)       | 0.0205<br>(0.62)     |
| Analyst coverage                           | 0.0059<br>(1.41)       | 0.0061<br>(1.56)      | -0.0042*<br>(-1.70)    | -0.0037<br>(-1.52)   |
| Loss dummy                                 | 0.0066<br>(1.10)       | 0.0038<br>(0.68)      | 0.0039<br>(0.93)       | 0.0042<br>(0.94)     |
| Liquidity                                  | 0.0060**<br>(2.28)     | 0.0071**<br>(2.56)    | 0.0104***<br>(4.45)    | 0.0099***<br>(4.14)  |
| Book-to-market                             | 0.0156***<br>(2.61)    | 0.0162***<br>(2.64)   | -0.0123***<br>(-2.82)  | -0.0119**<br>(-2.53) |
| Listing age                                | -0.0028<br>(-0.83)     | -0.0030<br>(-0.90)    | -0.0017<br>(-0.68)     | -0.0033<br>(-1.19)   |
| FY2023                                     | 0.0190***<br>(7.79)    | 0.0200***<br>(8.55)   | 0.0205***<br>(11.05)   | 0.0211***<br>(10.52) |
| FY2024                                     | 0.0092***<br>(3.77)    | 0.0110***<br>(4.91)   | -0.0038***<br>(-3.43)  | -0.0032**<br>(-2.54) |
| Controls                                   | Yes                    | Yes                   | Yes                    | Yes                  |
| Year fixed effects                         | Yes                    | Yes                   | Yes                    | Yes                  |
| Firm-clustered SE                          | Yes                    | Yes                   | Yes                    | Yes                  |
| N                                          | 300                    | 300                   | 300                    | 300                  |
| Adjusted R <sup>2</sup>                    | .216                   | .240                  | .421                   | .402                 |

*Note.* The dependent variable is the CAPM-based cost of equity. Australia\_Dummy is omitted because these models are estimated separately within each country. Coefficients are reported with firm-clustered t-statistics in parentheses. \*, \*\*, and \*\*\* indicate significance at the 10%, 5%, and 1% levels, respectively.

## Appendix 4C. Robustness and Sensitivity Tests

**Table 4C.1**

*Alternative Financing Cost Robustness Using LSEG StarMine WACC*

| Model                                               | Term                                       | Coefficient<br>(t-statistic) | Clustered<br>SE | p-value | N   | Adjusted<br>R <sup>2</sup> |
|-----------------------------------------------------|--------------------------------------------|------------------------------|-----------------|---------|-----|----------------------------|
| LSEG aggregate<br>CSRDS                             | CSRDS score                                | -0.0005<br>(-0.71)           | 0.0007          | .475    | 600 | 0.132                      |
| LSEG R2 indicator                                   | R2 Cyber risk and business<br>consequences | -0.0079**<br>(-2.18)         | 0.0036          | .030    | 600 | 0.143                      |
| LSEG CSRDS ×<br>Australia                           | CSRDS score × Australia                    | 0.0013<br>(0.95)             | 0.0014          | .342    | 600 | 0.133                      |
| LSEG R2 × Australia                                 | R2 × Australia                             | 0.0088<br>(1.11)             | 0.0080          | .268    | 600 | 0.145                      |
| LSEG dimensions<br>jointly                          | Relevance dimension                        | -0.0039*<br>(-1.83)          | 0.0021          | .067    | 600 | 0.138                      |
| LSEG positive CSRDS<br>indicator                    | Positive CSRDS indicator                   | -0.0039<br>(-1.32)           | 0.0029          | .185    | 600 | 0.135                      |
| LSEG positive CSRDS<br>subsample aggregate<br>CSRDS | CSRDS score                                | 0.0004<br>(0.48)             | 0.0008          | .630    | 357 | 0.218                      |
| LSEG positive CSRDS<br>subsample R2                 | R2 Cyber risk and business<br>consequences | -0.0065<br>(-1.58)           | 0.0041          | .115    | 357 | 0.227                      |

*Note.* The dependent variable is LSEG StarMine WACC. The treatment of the single missing observation is explained in Section 4.5. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

**Table 4C.2***Winsorised CAPM Robustness Models*

| Model term                              | Original coefficient | Original p | Winsorised coefficient | Winsorised p | N   |
|-----------------------------------------|----------------------|------------|------------------------|--------------|-----|
| CSRDS score                             | 0.0003               | .748       | -0.0001                | .929         | 600 |
| Specificity                             | 0.0009               | .519       | 0.0006                 | .651         | 600 |
| Relevance                               | -0.0032              | .178       | -0.0026                | .256         | 600 |
| Usefulness                              | 0.0058               | .258       | 0.0028                 | .394         | 600 |
| R2 Cyber risk and business consequences | -0.0121***           | .005       | -0.0124***             | .002         | 600 |
| CSRDS score × Australia                 | -0.0011              | .584       | -0.0019                | .214         | 600 |

*Note.* The dependent variable is CAPM-based cost of equity. Continuous variables are winsorised at the 1st and 99th percentiles where available. This table reports key coefficient-level robustness comparisons rather than full model output. \*, \*\*, and \*\*\* indicate significance at the 10%, 5%, and 1% levels, respectively.

**Table 4C.3***Positive CSRDS Indicator and Positive CSRDS Subsample Analyses*

| Model                                   | Sample         | Coefficient | Clustered SE | t/z   | p    | N   | Adj. R <sup>2</sup> |
|-----------------------------------------|----------------|-------------|--------------|-------|------|-----|---------------------|
| CAPM: positive CSRDS indicator          | Full sample    | -0.0038     | 0.0030       | -1.25 | .210 | 600 | .248                |
| CAPM: CSRDS score among disclosers      | CSRDS > 0 only | 0.0019      | 0.0012       | 1.60  | .110 | 357 | .228                |
| CAPM: R2 among disclosers               | CSRDS > 0 only | -0.0097**   | 0.0042       | -2.33 | .020 | 357 | .231                |
| LSEG WACC: positive CSRDS indicator     | Full sample    | -0.0039     | 0.0029       | -1.32 | .185 | 600 | .135                |
| LSEG WACC: CSRDS score among disclosers | CSRDS > 0 only | 0.0004      | 0.0008       | 0.48  | .630 | 357 | .218                |
| LSEG WACC: R2 among disclosers          | CSRDS > 0 only | -0.0065     | 0.0041       | -1.58 | .115 | 357 | .227                |

*Note.* The full sample models use a positive CSRDS indicator equal to one when at least one CSRDS indicator receives a positive score and zero otherwise. The restricted sample models are estimated using firm year observations with a CSRDS score greater than zero. A positive CSRDS score should not be interpreted as a general measure of disclosure existence. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

Table 4C.4

*Governance-Control Robustness Models*

| Dependent variable | Target variable                          | Baseline coefficient<br>(t-statistic) | Baseline p | With governance coefficient<br>(t-statistic) | With governance p | N   | Firms | Baseline Adj. R <sup>2</sup> | With governance adjusted R <sup>2</sup> |
|--------------------|------------------------------------------|---------------------------------------|------------|----------------------------------------------|-------------------|-----|-------|------------------------------|-----------------------------------------|
| CAPM CoE           | CSRDS score                              | -0.0004<br>(-0.26)                    | .794       | 0.0003<br>(0.16)                             | .871              | 293 | 102   | .249                         | .271                                    |
| CAPM CoE           | R2: cyber risk and business consequences | -0.0173***<br>(-3.55)                 | < .001     | -0.0157***<br>(-3.13)                        | .002              | 293 | 102   | .295                         | .308                                    |
| CAPM CoE           | Specificity dimension                    | 0.0004<br>(0.20)                      | .844       | 0.0011<br>(0.52)                             | .606              | 293 | 102   | .265                         | .286                                    |
| CAPM CoE           | Relevance dimension                      | -0.0055*<br>(-1.74)                   | .082       | -0.0048<br>(-1.50)                           | .133              | 293 | 102   | .265                         | .286                                    |
| CAPM CoE           | Usefulness dimension                     | 0.0065<br>(1.08)                      | .281       | 0.0066<br>(1.15)                             | .249              | 293 | 102   | .265                         | .286                                    |
| LSEG<br>WACC       | CSRDS score                              | -0.0004<br>(-0.32)                    | .748       | 0.0002<br>(0.18)                             | .860              | 293 | 102   | .185                         | .208                                    |
| LSEG<br>WACC       | R2: cyber risk and business consequences | -0.0077<br>(-1.46)                    | .143       | -0.0062<br>(-1.11)                           | .266              | 293 | 102   | .196                         | .215                                    |
| LSEG<br>WACC       | Specificity dimension                    | 0.0029*<br>(1.66)                     | .096       | 0.0035*<br>(1.93)                            | .054              | 293 | 102   | .211                         | .235                                    |

|      |            |           |      |           |      |     |     |      |      |
|------|------------|-----------|------|-----------|------|-----|-----|------|------|
| LSEG | Relevance  | -0.0061** | .019 | -0.0054** | .039 | 293 | 102 | .211 | .235 |
| WACC | dimension  | (-2.34)   |      | (-2.07)   |      |     |     |      |      |
| LSEG | Usefulness | -0.0014   | .763 | -0.0014   | .767 | 293 | 102 | .211 | .235 |
| WACC | dimension  | (-0.30)   |      | (-0.30)   |      |     |     |      |      |

*Note.* This table reports selected coefficients from governance subsample robustness models. The baseline models are estimated using the same 293 firm year observations but exclude board independence and board size. The governance augmented models add these two governance variables. All specifications include the Australia indicator, the firm level controls, fiscal year fixed effects, and firm clustered standard errors. Specificity, Relevance, and Usefulness are entered jointly in the dimension models; therefore, the corresponding model fit statistics are identical across the three dimension rows. The final two columns report adjusted R<sup>2</sup> for the baseline and governance augmented models, respectively. \*, \*\*, and \*\*\* indicate statistical significance at the 10 per cent, 5 per cent, and 1 per cent levels, respectively.

## Appendix 4D. Regression Diagnostics

**Table 4D.1**

### *Variance Inflation Factors for Final Regression Models*

| <b>Panel A. CAPM models</b>               |                       |                        |                        |                     |                     |
|-------------------------------------------|-----------------------|------------------------|------------------------|---------------------|---------------------|
| <b>Variable</b>                           | <b>CAPM aggregate</b> | <b>CAPM dimensions</b> | <b>CAPM indicators</b> | <b>CAPM R2 only</b> | <b>CAPM R2 × AU</b> |
| CSRDS score                               | 1.31                  |                        |                        |                     |                     |
| Specificity                               |                       | 1.81                   |                        |                     |                     |
| Relevance                                 |                       | 1.72                   |                        |                     |                     |
| Usefulness                                |                       | 1.31                   |                        |                     |                     |
| S1 Specific cyber threats                 |                       |                        | 1.73                   |                     |                     |
| S2 Cyber resilience and readiness         |                       |                        | 1.57                   |                     |                     |
| S3 Cyber risks to key assets              |                       |                        | 1.61                   |                     |                     |
| R1 Active cyber governance                |                       |                        | 1.35                   |                     |                     |
| R2 Cyber risk and business consequences   |                       |                        | 1.82                   | 1.51                | 6.06                |
| R3 Third-party and compliance cyber risks |                       |                        | 1.31                   |                     |                     |
| U1 Quantified cybersecurity resources     |                       |                        | 1.13                   |                     |                     |
| U2 Cyber insurance and exposure           |                       |                        | 1.14                   |                     |                     |
| U3 Cybersecurity performance metrics      |                       |                        | 1.23                   |                     |                     |
| Australia                                 | 4.18                  | 4.20                   | 5.10                   | 4.58                | 5.14                |
| R2 × Australia                            |                       |                        |                        |                     | 7.16                |
| Firm size                                 | 2.85                  | 2.90                   | 2.95                   | 2.84                | 2.84                |
| Leverage                                  | 1.40                  | 1.42                   | 1.45                   | 1.41                | 1.41                |
| ROA                                       | 1.59                  | 1.60                   | 1.62                   | 1.59                | 1.60                |
| Earnings volatility                       | 1.26                  | 1.27                   | 1.28                   | 1.27                | 1.27                |
| Analyst coverage                          | 2.51                  | 2.53                   | 2.56                   | 2.48                | 2.49                |
| Loss dummy                                | 1.73                  | 1.74                   | 1.78                   | 1.75                | 1.76                |
| Liquidity                                 | 3.65                  | 3.67                   | 3.88                   | 3.76                | 3.80                |
| Book-to-market                            | 1.39                  | 1.39                   | 1.42                   | 1.39                | 1.43                |
| Listing age                               | 1.39                  | 1.39                   | 1.41                   | 1.35                | 1.35                |
| FY2023                                    | 1.52                  | 1.53                   | 1.55                   | 1.51                | 1.51                |
| FY2024                                    | 1.43                  | 1.45                   | 1.47                   | 1.43                | 1.43                |
| <b>Panel B. LSEG WACC models</b>          |                       |                        |                        |                     |                     |
| <b>Variable</b>                           | <b>LSEG aggregate</b> | <b>LSEG dimensions</b> | <b>LSEG indicators</b> | <b>LSEG R2 only</b> | <b>LSEG R2 × AU</b> |
| CSRDS score                               | 1.32                  |                        |                        |                     |                     |
| Specificity                               |                       | 1.82                   |                        |                     |                     |
| Relevance                                 |                       | 1.72                   |                        |                     |                     |
| Usefulness                                |                       | 1.31                   |                        |                     |                     |
| S1 Specific cyber threats                 |                       |                        | 1.73                   |                     |                     |
| S2 Cyber resilience and readiness         |                       |                        | 1.57                   |                     |                     |
| S3 Cyber risks to key assets              |                       |                        | 1.61                   |                     |                     |
| R1 Active cyber governance                |                       |                        | 1.35                   |                     |                     |
| R2 Cyber risk and business consequences   |                       |                        | 1.82                   | 1.52                | 6.06                |

R3 Third-party and compliance cyber risks 1.31

**Panel B. LSEG WACC models**

| Variable                              | LSEG aggregate | LSEG dimensions | LSEG indicators | LSEG R2 only | LSEG R2 × AU |
|---------------------------------------|----------------|-----------------|-----------------|--------------|--------------|
| U1 Quantified cybersecurity resources |                |                 | 1.13            |              |              |
| U2 Cyber insurance and exposure       |                |                 | 1.14            |              |              |
| U3 Cybersecurity performance metrics  |                |                 | 1.23            |              |              |
| Australia                             | 4.18           | 4.20            | 5.09            | 4.58         | 5.13         |
| R2 × Australia                        |                |                 |                 |              | 7.16         |
| Firm size                             | 2.85           | 2.90            | 2.95            | 2.84         | 2.84         |
| Leverage                              | 1.41           | 1.43            | 1.45            | 1.41         | 1.42         |
| ROA                                   | 1.59           | 1.60            | 1.62            | 1.59         | 1.60         |
| Earnings volatility                   | 1.26           | 1.27            | 1.28            | 1.27         | 1.27         |
| Analyst coverage                      | 2.52           | 2.54            | 2.57            | 2.49         | 2.50         |
| Loss dummy                            | 1.73           | 1.74            | 1.78            | 1.75         | 1.76         |
| Liquidity                             | 3.64           | 3.66            | 3.87            | 3.74         | 3.78         |
| Book-to-market                        | 1.38           | 1.39            | 1.42            | 1.39         | 1.43         |
| Listing age                           | 1.40           | 1.40            | 1.42            | 1.35         | 1.36         |
| FY2023                                | 1.52           | 1.54            | 1.55            | 1.51         | 1.51         |
| FY2024                                | 1.43           | 1.46            | 1.47            | 1.43         | 1.43         |

*Note.* This table reports VIF diagnostics for the final regression specifications. VIF values below 5 are generally considered acceptable, while values below 10 are not normally regarded as severe multicollinearity. The higher VIFs in the interaction models arise mechanically from the inclusion of interaction terms and their component variables.