

Cybersecurity disclosure: Board commitment and regulatory impact in the UK

Elmarzouky, M., Moussa, T. and Allam, A.

Electronic version of an article published as Elmarzouky, M., Moussa, T. and Allam, A. 2025. Cybersecurity disclosure: Board commitment and regulatory impact in the UK. The International Journal of Accounting. Advanced online publication.

<https://doi.org/10.1142/S1094406025420053>

© Copyright World Scientific Publishing Company [Journal URL]

The final definitive version is online at:

<https://doi.org/10.1142/S1094406025420053>

The WestminsterResearch online digital archive at the University of Westminster aims to make the research output of the University available to a wider audience. Copyright and Moral Rights remain with the authors and/or copyright owners.

Cybersecurity disclosure: Board commitment and regulatory impact in the UK

Mahmoud Elmarzouky

University of St Andrews Business School
University of St Andrews, St Andrews, Fife, KY16 9AJ, United Kingdom
mahmoud.elmarzouky@st-andrews.ac.uk

Tantawy Moussa

School of Finance and Accounting
University of Westminster, London, United Kingdom
t.moussa@westminster.ac.uk

Amir Allam

Aston Business School
Aston University, Birmingham, United Kingdom
a.allam@aston.ac.uk

Accepted for Publication on 20 April 2025

This article should be cited as follows:

Elmarzouky, M., Moussa, T. and Allam, A., 2025. Cybersecurity disclosure: Board commitment and regulatory impact in the UK. *The International Journal of Accounting*, forthcoming.

Synopsis

The Research Problem

This study investigates the relationship between board commitment to cybersecurity governance (BCCG) and corporate cybersecurity disclosures (CSD) in the UK. It focuses on how the UK's Network and Information Systems (NIS) 2018 regulation influences this relationship, considering cyber threats' rising complexity and frequency.

Motivation

With the digital age's escalating cybersecurity threats, strong cybersecurity governance and transparent disclosure practices have become crucial. The study seeks to understand whether a board's commitment to cybersecurity, particularly in the context of the NIS regulation, affects the extent of a company's CSD.

The Test Hypotheses

This study tests two hypotheses. The first hypothesis posits a positive association between BCCG and the extent of CSD. The second hypothesis contends that the UK's NIS 2018 regulation positively moderates the relationship between board commitment and CSD.

Target Population

This study should be of interest to boards of directors, policymakers, regulators, and various stakeholder groups.

Adopted Methodology

The study employed textual analysis using Python to analyze corporate disclosures, fixed effect regressions, Difference-in-Differences (DID), and Propensity Score Matching analyses.

Analyses

We examined the relationship between BCCG and CSD against the backdrop of the UK's NIS 2018 regulation. We first assessed the extent of CSD in the UK FTSE 350 firms using Python-based textual analysis. Then, we conducted a regression analysis to assess the impact of BCCG on CSD and the moderating effect of the NIS regulation. This was complemented by a DiD analysis to evaluate the changes in CSD before and after the introduction of the NIS regulation.

Findings

We find that BCCG is positively associated with the extent of CSD, and that the NIS regulation positively moderates this relationship. Our evidence suggests that firms with a greater focus on cybersecurity governance at the board level (e.g., directors with IT expertise, the presence of IT committees and cybersecurity policies) demonstrate a higher commitment to managing and reporting cybersecurity risks and solutions. Moreover, using DiD analysis, we find a significant increase in CSD levels among firms subjected to NIS regulation compared to control firms, post-NIS regulation. Overall, our study suggests that the interplay of BCCG and macro-social factors, such as NIS regulation, enhances firms' sensitivity to institutional and stakeholder pressures, leading them to increase their corporate CSD.

Keywords: Cybersecurity disclosure, board commitment, NIS regulation, Python, Textual analysis, UK.

1. Introduction

In the contemporary digital landscape, where technology infrastructures form the backbone of global economic and social frameworks, the significance of robust cybersecurity governance is increasingly emphasized. Cybersecurity threats pose a significant and growing risk (Florackis et al., 2023; Kamiya et al., 2021; Lankton et al., 2021; Rosati et al., 2019; Zhang, 2024) and range from minor data breaches to extensive cyberattacks capable of paralyzing entire systems.¹ In response to these growing threats, the UK's Network and Information Systems (NIS) 2018 regulation was introduced as a pivotal initiative safeguard critical services and strengthen organizational commitment to cybersecurity.

¹ The financial implications are substantial, with the average cost of a data breach in the UK estimated at approximately 4.53 million USD, just below the global average of 4.88 million USD (IBM, 2024). Firms with increased cybersecurity risks are charged higher audit fees (Rosati et al., 2019). The increase in cybersecurity risk is shaping corporate innovation, including firms' efforts to protect their intellectual capital, potentially negatively impacting research and development spending (Lattanzio & Ma, 2023).

The regulation addresses critical cybersecurity challenges by targeting operators of essential services and digital service providers in sectors such as energy, transport, water, healthcare, and digital infrastructure.² It mandates stringent cybersecurity protocols, imposes penalties for non-compliance, and requires organizations to adopt technical and organizational measures to mitigate risks and minimize security incidents.³ Implemented in May 2018 with a phased approach, the regulation highlights the need for comprehensive cybersecurity governance and transparent disclosure practices, extending beyond technical solutions.

In response to this regulatory pressure, corporate boards have been compelled to develop robust cybersecurity strategies by integrating cybersecurity expertise at the board level, fostering a strategic approach to managing cybersecurity risks, and ensuring transparent and comprehensive disclosure of cybersecurity measures and incidents. Such proactive engagement addresses the evolving expectations of stakeholders, who increasingly demand deeper insights into firms' cybersecurity preparedness and response strategies (Gao et al., 2020; Radu & Smaili, 2022; Smaili et al., 2023). Zhang (2024) underscores how firms with heightened cybersecurity risks often adopt proactive strategies, such as CSR, to bolster their reputation and mitigate the adverse consequences of potential data breaches, aligning with stakeholder expectations.

Corporate disclosure significantly influences financial markets (Cao et al., 2021). Cybersecurity disclosures are particularly important because they maintain stakeholder trust

² Digital infrastructure includes digital service providers such as search engines, cloud computing services, and online marketplaces, which play a significant role in the digital economy.

³ For example, failing to implement appropriate security measures can result in a fine of up to £17 million or a percentage of global turnover, depending on which is higher.

and ensure market stability. While recent studies address cybersecurity disclosure (Calderon & Gao, 2021, 2022; Chen et al., 2023; Gao et al., 2020; Li et al., 2018), limited research explores how corporate governance impacts these disclosures (Radu & Smaili, 2022; Smaili et al., 2023; Trinh et al., 2024). This gap highlights the need to examine how board commitment to cybersecurity governance (BCCG) shapes disclosure amid evolving cyber threats, especially within regulated environments like the NIS framework.

To address this gap, our study integrates resource dependence theory (RDT), stakeholder theory, and institutional theory to investigate the relationship between BCCG and the extent of cybersecurity disclosure, while also examining the moderating effect of the NIS regulation. The FTSE 350 serves as an ideal study setting due to these companies' critical role in the UK's economic framework and their exposure to the stringent regulatory requirements imposed by the NIS regulation.

This environment offers a valuable opportunity to explore how regulatory frameworks interact with corporate governance to improve cybersecurity transparency and accountability across industries. Examining the FTSE 350 reveals the complexity of such disclosures and provides insights into how aligning governance mechanisms with regulatory expectations enhances transparency, compliance, and stakeholder trust.

Our study uses an innovative methodology to measure corporate cybersecurity disclosures (CSD) through Python-based textual analysis of FTSE 350 annual reports from 2015-2021. CSD is categorized into two groups: cybersecurity threats and incidents (CSTI) and cybersecurity risk mitigation and technologies (CRMT). CSTI evaluates a firm's transparency

regarding potential and existing cybersecurity threats, while CRMT assesses the disclosure of strategies and technologies for risk prevention. Each category is quantified as the percentage of relevant sentences in annual reports, identified using a comprehensive keyword list from prior research.

We assess BCCG using a composite measure that includes the presence of a cybersecurity policy, a board IT committee, and IT expertise among board members. Unlike prior studies relying on single attributes, this approach captures the board's collective judgment (Desender et al., 2016; Jain & Zaman, 2020). Each element contributes to the BCCG score, reflecting a firm's overall commitment to cybersecurity. This framework enables a robust analysis of the interaction between BCCG and CSD under the stringent NIS Regulation of 2018.

We find a positive association between BCCG and CSD. Using a difference-in-differences (DiD) design, our analysis shows a significant increase in CSD levels among firms subject to the NIS regulation compared to control firms post-regulation, illustrating how firms respond by enhancing disclosures. The NIS regulation also positively moderates the BCCG-CSD relationship, demonstrating synergy between governance and regulatory compliance. Notably, a lack of IT expertise among female and independent directors underscores the need for greater diversity in board skills.

This study contributes to the literature by providing empirical evidence on the relationship between BCCG and CSD levels, particularly within the regulated environment post-NIS. It is the first to examine the impact of the NIS regulation on CSD, highlighting how regulatory efficacy shapes corporate strategy. The finding that NIS moderates the BCCG-CSD

relationship underscores the effectiveness of regulatory interventions in enhancing corporate responses to cybersecurity risks, offering valuable insights for regulators and policymakers in shaping future cybersecurity policies.

Second, this paper advances the literature on corporate commitment to cybersecurity by introducing a comprehensive measure that captures the collective judgment of the board. Unlike studies focused on single attributes (e.g., Higgs et al., 2016; Lankton et al., 2021; Smaili et al., 2023; Wilkin & Chenhall, 2020), our measure incorporates multiple components, including the presence of a cybersecurity policy, a board IT committee, and IT expertise among board members. Relying solely on single proxies provides an incomplete view, whereas our approach considers additional factors to better reflect a firm's true commitment to cybersecurity. All data were meticulously and manually collected to ensure accuracy and relevance.

Third, a key contribution of this study is the use of Python for textual analysis of annual reports to measure CSD. This offers a methodologically sound and innovative approach to analyzing corporate disclosures. Additionally, this application sets the stage for future research to leverage advanced analytical techniques. Finally, by integrating insights from resource dependence, stakeholder, and institutional theories, the study also contributes to understanding how regulations like the NIS influence corporate behavior and governance in cybersecurity.

The findings of this study provide valuable insights for policymakers, corporate leaders, and stakeholders, highlighting the critical role of board commitment and expertise in improving CSD. Proactive board governance fosters comprehensive disclosures that meet regulatory

standards like the NIS regulation while promoting transparency and trust in financial markets. Greater transparency can mitigate the negative impact of cybersecurity risks on market value, protecting shareholder interests. These insights guide corporate strategies and regulatory policies in an increasingly digital and risk-prone environment, advocating for governance frameworks with enhanced cybersecurity competencies. By demonstrating the benefits of board-level expertise and regulatory adherence, this study supports the development of targeted interventions to strengthen cybersecurity practices across industries.

The remainder of the paper unfolds as follows: Section 2 discusses the research background and its theoretical framework. Section 3 presents the development of hypotheses. Section 4 describes the research methodology. Section 5 presents the empirical results and discussions, followed by additional analyses and robustness checks in Section 6. The final section concludes with insights into the implications of the findings, limitations, and directions for future research.

2. Background and theoretical framework

This study adopts a multi-theoretical framework to explore the relationships between BCCG, CSD, and the introduction of the NIS regulation. The complexity of these constructs necessitates a comprehensive approach that draws on RDT, stakeholder theory, and institutional theory.

Pfeffer and Salancik's (1978) RDT provides a lens through which to understand the link between BCCG and CSD. RDT emphasizes the board's expertise and knowledge in shaping strategic decisions (Mallin et al., 2013) by offering informed advice, building external

networks, and securing critical resources (Arena et al., 2015; Mallin & Michelon, 2011; Pfeffer & Salancik, 1978; Wang & Dewhirst, 1992). In the context of cybersecurity, boards with IT expertise are well-positioned to establish policies and IT committees, fostering a strategic focus on cybersecurity governance.

Stakeholder theory (Freeman, 2010) highlights the need to manage the stakeholder expectations, as they control resources critical to the firm (Fernando & Lawrence, 2014; Helfaya & Moussa, 2017; Helfaya & Whittington, 2019; Mallin et al., 2013). Stakeholders demand assurance through transparent disclosures that cybersecurity risks are effectively managed (Radu & Smaili, 2022; Walton et al., 2021). Actions like having IT expertise on the boards, dedicated IT committees, and cybersecurity policies are pivotal in building trust, mitigating concerns, and enhancing reputation (Kamiya et al., 2021). Thus, stakeholder theory underscores the role of BCCG in fostering comprehensive disclosures to address diverse stakeholder interests.

Finally, when considering the impact of regulation on CSD, the institutional theory (DiMaggio & Powell, 1983) provides a theoretical lens to understand the influence of regulations on the firm's behavior. It posits that organizations tend to conform to the norms and rules established in their institutional environment to gain legitimacy (North, 1990). In the context of cybersecurity, this theory suggests that the introduction of the NIS regulation compels firms to enhance their commitment to cybersecurity governance and, accordingly, disclosure.

3. Hypotheses development

3.1. Board commitment to cybersecurity governance and cybersecurity disclosure levels

The role of board commitment in shaping disclosure practices has been well-documented in corporate governance research (e.g., Albitar et al., 2023; Ben-Amar & Belgacem, 2018; Pae & Choi, 2011; Salin et al., 2019). As the key decision-making entity, the board influences a firm's commitment to areas like cybersecurity governance and disclosure. For instance, losses to shareholder wealth are lower when boards emphasize risk management proactively, particularly before cyber-attacks (Kamiya et al., 2021).

As an essential sign of board commitment, adequate board composition is critical for board effectiveness (Mallin et al., 2013; Minichilli et al., 2009) and is positively associated with various metrics of corporate performance and reputation (e.g., Gull et al., 2018; Lanis & Richardson, 2011; Post & Byron, 2015; Wahid, 2019). In particular, members' expertise is considered essential for optimal performance and the quality of strategic decisions (Carter & Lorsch, 2003; McIntyre et al., 2007).

From an RDT perspective, experienced boards leverage their expertise to access resources and networks (Pfeffer & Salancik, 1978), enabling robust cybersecurity measures and improved disclosure (Arena et al., 2015; Mallin & Michelon, 2011; Wang & Dewhirst, 1992). Stakeholder theory further underscores the importance of transparency in addressing the growing stakeholders' concerns over cybersecurity risks (Freeman, 2010; Radu & Smaili, 2022; Walton et al., 2021).

Empirical evidence supports these theoretical perspectives. Firms with strong governance disclose more information on cybersecurity (Amir et al., 2018; Haislip et al., 2020; Smaili et al., 2023). Such disclosure enhances transparency and timeliness in corporate communication while fostering stakeholder trust and confidence in the firm's capability to effectively manage cybersecurity risks. (Haislip et al., 2020). Amir et al. (2018) found firms with weaker corporate governance are more likely to withhold information on cyber-attacks compared to those with stronger governance. Smaili et al (2023) provided evidence of increased CSD in firms with higher board effectiveness. Board IT expertise and the presence of technology committees are particularly associated with greater CSD, including risk mitigation and breach reporting (Héroux & Fortin, 2022; Higgs et al., 2016; Lankton et al., 2021). Therefore, integrating insights from RDT and stakeholder theory, along with supporting empirical evidence, our first hypothesis is formulated as follows:

H₁: Board commitment to cybersecurity governance positively influences cybersecurity disclosure.

3.2. The moderating role of the NIS regulation

As new challenges arise, increased disclosure is often necessary to address the stakeholder concerns. Regulatory pressures, such as those imposed by the NIS regulation, play a key role in shaping corporate priorities, particularly in cybersecurity. The NIS requires firms to take measures to manage cybersecurity risks, and it mandates the reporting of security incidents within 72 hours (NIS, 2018), underscoring the importance of transparency and disclosure.

Research demonstrates that regulation significantly impacts corporate disclosures, though effects vary. For example, the UK's 2006 Companies Act increased disclosures on emissions,

gender, and human rights (Hummel & Rötzel, 2019), while the US SEC's Regulation G improved credit ratings for debt issuers (Thielemann et al., 2019). Conversely, some regulations, like the California Transparency in Supply Chains Act and the UK Modern Slavery Act, yielded more symbolic than substantive disclosures (Allam et al., 2024; Birkey et al., 2018; Moussa et al., 2023; Rogerson et al., 2020).

From an institutional theory perspective, the NIS regulation signals the importance of cybersecurity, encouraging firms to enhance disclosures to exhibit conformity and gain legitimacy (DiMaggio & Powell, 1983). Similarly, RDT suggests that regulatory pressures drive boards to acquire resources, such as IT expertise, to comply with mandates, thereby improving CSD (Bravo & Alcaide-Ruiz, 2019; Masud et al., 2019; Naheed et al., 2021; Pfeffer & Salancik, 1978; Shahab et al., 2020).

Stakeholder theory further explains the moderating role of the NIS regulation on the relationship between BCCG and disclosure. By addressing broader stakeholder expectations (Markopoulou et al., 2019), the NIS sets standards for cybersecurity practices and influences communication. In firms with high BCCG, compliance with NIS enhances the quality of disclosures, effectively addressing stakeholders' informational needs (Héroux & Fortin, 2022). Thus, the NIS regulation directly influences CSD while also magnifying the impact of BCCG. This interplay between governance and regulatory environments leads to the following hypotheses:

H₂: The introduction of the NIS regulation positively influences cybersecurity disclosure.

H₃: NIS moderates the relationship between board commitment to cybersecurity and cybersecurity disclosure.

Figure 1 demonstrates our theoretical model, including the main variables and the hypothesized relationships.

[Insert Figure 1]

4. Research Design

4.1. Data and sample

Table 1 summarizes our sample selection and its industry-wise distribution of the sample. We began with 2,450 firm-year observations of UK FTSE 350 firms from 2015 through 2021, allowing us to fully exploit variations in CSD and BCCG. We excluded 210 observations with a missing firm annual report. We further excluded 363 observations for which BCCG, and other variables' data were unavailable. The final sample consisted of 1,877 firm-year observations for the analysis. Table 1 also displays the industry-wise distribution of the sample, encompassing various categories of firms rather than just large ones. The subsequent breakdown of the final sample into distinct industries reveals the composition, with Financials constituting the largest proportion (36%), followed by Industrials (18%) and Consumer Discretionary (15%). Both corporate CSD and BCCG data were manually collected from the firms' annual reports, which we obtained from annualreport.com or, if unavailable for a specific year, directly from the firm's official website. Financial and corporate governance data were sourced from the DataStream database.

[Insert Table 1]

4.2. Measures of CSD

The primary dependent variable in this study is the extent of disclosed cybersecurity information, termed CSD, and is measured as the proportion of sentences in a firm's annual report relating to CSD, scaled against the total number of sentences in the report (e.g., Chen et

al., 2023; Florackis et al., 2023; Gao et al., 2020). Sentences offer a more reliable basis for coding than other units of analysis. They are straightforward to identify and exhibit less variation between researchers compared to phrases, clauses, or themes (Florackis et al., 2023; Hasseldine et al., 2005). Following prior studies (Elnahass et al., 2024; Gao et al., 2020; Gordon et al., 2010; Li et al., 2018; Radu & Smaili, 2022; Smaili et al., 2023), we employed textual analysis to capture the levels of CSD among UK companies.

To conduct the textual analysis, we first collected all available annual reports for UK FTSE 350 firms. We then extracted sentences related to CSD using a comprehensive list of keywords and bigrams, including terms like 'cyber attack', 'cyber fraud', 'cyber threat', 'cyber criminals', 'security breach', 'unauthorised access', 'hacking', 'social engineering', and 'cyber insurance'. The complete list of keywords used to identify CSD is provided in Appendix 2. We categorized the overall CSD into two groups: Cybersecurity Threats and Incidents (CSTI) and Cybersecurity Risk Mitigation and Technologies (CRMT). CSTI assesses a firm's transparency in disclosing potential and existing cybersecurity threats, offering insights into the cybersecurity challenges that could impact stakeholders. For example, BT Group Plc (2018, p. 51) annual report stated: "We have compartmentalised our IT estate as we provision new cloud-based systems to limit the potential impact of a cyber attack." On the other hand, CRMT evaluates the transparency regarding a firm's efforts to mitigate cybersecurity risks, reflecting how companies communicate their proactive strategies and investments in cybersecurity technologies. For example, Marshall Plc (2021, p. 38) annual report declared: "Appropriate tools and training procedures are in place to protect sensitive data when stored and transmitted between parties (e.g. encryption of hard drives, restricted USB devices, secure data

transmission mechanisms and third-party security audits).” More examples of excerpts from annual reports that reference CSD can be found in Appendix 3.

To ensure the reliability and validity of the CSD measures, we followed several verification steps from prior research (e.g., Collis & Hussey, 2021; Elnahass et al., 2024; Florackis et al., 2023; Krippendorff, 2018; Loughran & McDonald, 2011). Initially, we sought expert validation by engaging specialists in cybersecurity and corporate disclosures to review our keyword list (Collis & Hussey, 2021). This expert review was crucial in confirming that the list comprehensively captured all relevant aspects of cybersecurity risk disclosures, thereby enhancing the content validity of our measure. Following this, we conducted a pilot test involving a random sample of 10 companies from the FTSE 350. We manually counted cybersecurity-related sentences in these companies' annual reports using the word count function in PDF files. These manual counts were then compared with results from our Python-based extraction process, and the results showed consistent accuracy. To illustrate the reliability of our measures, we included examples of CSD excerpts in Appendix 3. These examples illustrate our methodology and ensure that our proxies accurately reflect the breadth and depth of CSD.

Our analysis also integrated sensitivity tests using alternative proxies for CSD. Specifically, we employed a bag-of-words approach to measure the frequency of cybersecurity-related words in the annual report. This widely accepted method in textual analysis leverages robust text-processing capabilities to isolate and extract relevant information from large volumes of text (Campbell, 2004; Loughran & McDonald, 2011; Smaili et al., 2023). Additionally, we constructed an alternative CSD proxy to assess the firm's propensity to disclose cybersecurity

information, following prior research (Ben-Amar & McIlkenny, 2015; Smaili et al., 2023). This proxy is represented as a dichotomous variable, where a value of one is assigned if the firm disclosed cybersecurity information, and zero if it did not.

4.3. Measures of BCCG

To capture the extent of board commitment in overseeing and reporting on cybersecurity risks and practices, we employed a composite measure that integrates various cybersecurity and IT-related board attributes. This approach contrasts with studies that focus on single board attributes, as it evaluates the collective judgment of the board (Desender et al., 2016; Jain & Zaman, 2020). Our composite measure includes elements such as the existence of a cybersecurity policy, a board IT committee, and the IT expertise of board members, with a particular emphasis on female and independent directors possessing IT expertise (e.g., Higgs et al., 2016; Lankton et al., 2021; Smaili et al., 2023; Wilkin & Chenhall, 2020). Prior research suggests that diverse boards are more effective in risk management. Female directors and independent directors are often seen as more cautious and risk-aware, qualities that are crucial for overseeing cybersecurity risks and strategies (Elnahass et al., 2024; Smaili et al., 2023).

The assessment of each director's IT expertise involves evaluating their professional background in IT roles, previous board memberships in the Information and Communication Technology (ICT) industries, academic credentials in IT-related fields (such as computer science, management information systems, and computer information systems) at various levels (Bachelor's, Master's, Ph.D.), professional certifications (e.g., CISM, CISSP, OSCP), and participation in technology-related initiatives such as big data analytics, digital transformation, cloud computing, cybersecurity programs, AI, and fintech.

To ensure the reliability of our manually collected data on board members' IT expertise, we implemented a rigorous multi-stage verification process that began with a pilot study on a subset of 10 companies, allowing us to refine our data collection procedures before expanding to the full sample. Following this, the board of directors' expertise data was independently coded by team members and subsequently double-checked by another member to minimize subjectivity and ensure accuracy. We further validated our approach by conducting inter-coder reliability tests, where multiple researchers independently coded a random sample of the board members' data, yielding a high inter-coder agreement of 93%, with a Cohen's Kappa coefficient exceeding 0.85, indicating strong reliability in our coding process (Cohen, 1960). Moreover, we conducted periodic reliability checks throughout the data collection process to maintain ongoing accuracy and consistency. These checks revealed no significant variances, affirming the replicability of our results (Krippendorff, 2018). This comprehensive approach, encompassing pilot testing, double-checking, inter-coder reliability assessments, and continuous monitoring, ensures that our BCCG measure is both robust and reliable.

To develop the composite BCCG measure, we apply Principal Component Analysis (PCA), a method that is widely used in prior studies (e.g., Arena et al., 2015; Elamer et al., 2020; Mallin et al., 2013; Tunyi & Ntim, 2016). PCA helps reduce data dimensionality while enhancing interpretability. The analysis yields a Kaiser–Meyer–Olkin (KMO) measure of 0.842, which exceeds the recommended threshold of 0.50, indicating the appropriateness of PCA for this data. The resulting composite BCCG measure reflects the board's comprehensive approach to cybersecurity governance, capturing not only the presence of formal structures and policies but also the depth of IT expertise on the board. This measure also emphasizes the

diversity of board expertise, which enhances the quality of decision-making and risk assessment (Arena et al., 2015; Mallin et al., 2013).

In addition to the PCA-based measure, we develop an alternative BCCG measure following the methodology of Albitar et al. (2023). This alternative measure aggregates five cybersecurity and IT-related board attributes. Specifically, the presence of a cybersecurity policy and a board IT committee are treated as dummy variables, scored as 1 if present and 0 otherwise. The IT expertise of board members, female directors, and independent directors are scored based on whether they exceed the median values in these areas, with a score of 1 for above median and 0 otherwise. This scoring system quantifies BCCG on a scale from 0 to 5, providing a comprehensive indicator of the board's commitment to cybersecurity.

4.4. NIS regulation

This study investigated the impact of the NIS Regulation 2018, which is aimed at enhancing the security and resilience, both cyber and physical, of critical network and information systems necessary for providing essential and digital services. For this purpose, we employed the NIS as a dummy variable, assigned a value of 1 for the post-2018 period (covering the years 2019 to 2021) and 0 for the 2015-18 period.

4.5. Controls

To account for the confounding effects of firm-specific characteristics and governance mechanisms that may influence BCCG and CSD, we incorporated several control variables, drawing on prior studies (e.g., Gao et al., 2020; Higgs et al., 2016; Hilary et al., 2016; Lankton et al., 2021; Smaili et al., 2023). These variables include firm characteristics such as firm size

(FSIZE), profitability (ROE), leverage (LEV), asset tangibility (INTAN), presence of losses (LOSS), and growth opportunities (MTBV). For example, prior research (Gao et al., 2020; Hilary et al., 2016) indicates that larger firms and those with lower market-to-book ratios tend to disclose more information about cybersecurity risks, whereas highly leveraged firms are less likely to mention these risks in annual reports. Furthermore, governance mechanisms at the firm level are considered, including board size (BSIZE), independence (BINDE), and governance score (GOVS). Radu and Smaili (2022) indicated that the presence of women on boards positively impacts CSD; thus, we included gender diversity (BGD). We also accounted for the effects of the year and industry. Appendix 1 provides detailed definitions of all variables.

4.6. Empirical models

To investigate the impact of BCCG on CSD and assess the moderating effect of the NIS regulation on this relationship, we employed Ordinary Least Squares (OLS) regression with robust standard errors. The use of robust standard errors is crucial as it addresses issues of heteroscedasticity and non-independence of observations, which are common in panel data settings (Trinh et al., 2024; Wooldridge, 2010). Moreover, to control for unobserved time-invariant factors that may vary across years and industries, year-fixed effects and industry-fixed effects were incorporated into all models (Wooldridge, 2010). We also account for potential endogeneity by including governance and firm-level control variables, which helps to mitigate concerns related to omitted variable bias. The models estimated in our analysis are as follows.

$$CSD_{it} = \alpha_0 + \beta_1 BCCG_{it} + \sum_{i=1}^n \beta_i CONTROLS_{it} + \varepsilon_{it} \quad (1)$$

$$CSD_{it} = \alpha_0 + \beta_1 BCCG_{it} + \beta_2 NIS_{it} + \beta_3 BCCG_{it} * NIS_{it} +$$

$$\sum_{i=1}^n \beta_i \text{CONTROLS}_{it} + \varepsilon_{it} \quad (2)$$

where CSD_{it} is a proxy of the cybersecurity disclosure of firm i at time t , $BCCG_{it}$ is a composite indicator of the board commitment to cybersecurity governance, NIS_{it} indicates the impact of the 2018 Network and Information Systems regulation. This is measured by a dummy variable that takes the value 1 for the post-2018 period (covering the years 2018 to 2021) and 0 otherwise. $BCTCSD_{it} * NIS_{it}$ is the interaction term between $BCTCSD_{it}$ and NIS_{it} . $CONTROLS_{it}$ refers to a vector of firm-level control variables. All continuous variables are winsorized at the 1% and 99% levels to mitigate the influence of outliers. Detailed definitions of all variables are provided in Appendix 1.

To ensure the robustness of our results and address potential endogeneity concerns, we conducted several additional tests. First, we included one-year-lagged independent variables in our models to account for potential reverse causality, which helps to further mitigate endogeneity. This approach is complemented by the use of alternative proxies for both CSD and BCCG, ensuring that our findings are not driven by the specific operationalization of these constructs. Furthermore, we applied two-stage least squares (2SLS) and three-stage least squares (3SLS) estimation techniques to address potential endogeneity, particularly in simultaneous equation models within dynamic random effects contexts (Trinh et al., 2024; Zellner & Theil, 1992). Among these, 3SLS is considered more efficient than 2SLS because it accounts for cross-equation correlations and does not require a normal distribution of errors. Finally, we employed a DiD analysis and Propensity Score Matching (PSM), which helped to strengthen the causal inference of our findings.

5. Results

5.1. Descriptive statistics

Table 2 reports the descriptive statistics for all variables used in our study. On average, CSD constitutes 0.171% of the total sentences in the annual reports, with a standard deviation of 0.191%. The range of CSD percentages varies from 0% to a maximum of 3.256%. Regarding the number of sentences, firms, on average, dedicate approximately 9 sentences (mean = 8.998) to cybersecurity, with a significant variation (std. dev. = 11.354) across the sample, ranging from 0 to 144 sentences. This suggests that, on average, the disclosure of cybersecurity information in annual reports is minimal.

The results further indicate that, on average, only 0.037% of sentences in the annual reports are related to cybersecurity threats and incidents (CSTI), with some firms reporting as much as 0.690%, while others reporting none at all. This suggests that explicit information on threats and incidents is relatively infrequent in corporate disclosures. Similarly, the average percentage of sentences focusing on cybersecurity risk mitigation and technologies (CRMT) is 0.068%, with a range extending up to 1.895%, suggesting that while there is some focus on these areas, it remains modest.

In terms of board governance, 59.4% of the firms in the sample have a dedicated board IT committee (BITC), and 32.1% have a formal cybersecurity policy (FCSP). Furthermore, 15.7% of board members, on average, possess IT expertise (BITEXP), though this expertise is less prevalent among female (BDITEXP) (6.153%) and independent directors (BINDITEXP) (6.079%). This points to an area for potential improvement in board diversity concerning IT

skills. The results also reveal that the BCCG varies significantly, ranging from -1.628 to 5.767, with a standard deviation of 1.559.

[Insert Table 2]

Table 3 shows the mean values of CSD across industries over the sample period. The results indicate a significant increase in CSD across all industries from 2015 to 2021, with the average number of sentences rising from 4.419 to 14.603. The Telecommunications and Technology industries lead in CSD, with Telecommunications growing from 13.25 sentences in 2015 to 34.167 in 2021, and Technology from 2.857 to 35.5 sentences. This reflects these industries' high exposure to digital risks and the critical nature of their services. In contrast, Basic Materials and Real Estate report lower levels of CSD, despite showing growth. Basic Materials increased from 2.231 sentences in 2015 to 15.533 sentences in 2021, and Real Estate from 2.174 to 12.286 sentences. These industries' lower CSD may indicate a slower recognition of cybersecurity risks, potentially leaving them more vulnerable. Moreover, the overall rise in CSD, particularly post-2019, aligns with increased regulatory pressures and stakeholder demands for greater transparency in cybersecurity practices. However, the variation across industries suggests that some sectors still need to enhance their cybersecurity reporting to meet evolving expectations and mitigate risks effectively.

[Insert Table 3]

Table 4 presents the results of the Pearson correlation analysis conducted on all variables incorporated in our regression analyses. It is evident that BCCG has a positive correlation with CSD ($\beta = 0.373$, $p < 0.001$). We also observe a significant correlation between the presence of NIS regulation (NIS) and both CSD ($\beta = 0.200$, $p < 0.001$) and BCCG ($\beta = 0.334$, $p < 0.001$), suggesting that regulatory factors play a crucial role in shaping corporate CSD. Overall, these results are broadly in line with our hypotheses. Our correlation analysis also reveals low

correlation values among the independent and control variables, suggesting that multicollinearity is unlikely to be a significant issue. This is further supported by calculating Variance Inflation Factors (VIFs) for all independent variables in the multivariate regressions. The results (un-tabulated) show that all individual VIF values are below 2, and the mean VIF is well below the critical threshold of 6 (Marquardt, 1970). Therefore, we conclude that multicollinearity is not a concern in our estimations.

[Insert Table 4]

5.2. Empirical results

5.2.1. The impact of BCCG on CSD

Table 5 shows the results for the first study hypothesis, H1, assessing the relationship between BCCG and various aspects of corporate CSD, including overall CSD and its sub-categories CSTI and CRMT.

In Model 1, the coefficient for BCCG is positively and significantly associated with CSD ($\beta = 3.010$, $p < .001$), indicating that greater BCCG positively influences the level of cybersecurity information firms disclose. To understand the economic significance, we calculated the impact of a one standard deviation change in BCCG on CSD. The result shows that a one standard deviation increase in BCCG leads to an increase of approximately 0.4694 units in CSD. Given the mean of CSD is 0.171, this represents a substantial change, highlighting the strong economic impact of BCCG on corporate CSD.

In Models 2 and 3, which disaggregate CSD into CSTI and CRMT, BCCG continues to show a significant positive impact. Specifically, BCCG has a strong positive effect on CSTI

disclosures ($\beta = 0.442$, $p < 0.01$) and CRMT disclosures ($\beta = 0.736$, $p < 0.01$). These findings further support the pivotal role of committed boards in enhancing transparency across various dimensions of cybersecurity. The positive relationship between BCCG and CSTI disclosures suggests that boards committed to cybersecurity governance are more likely to ensure that firms are transparent about their exposure to cybersecurity threats and incidents. Similarly, the significant impact of BCCG on CRMT disclosures indicates that such boards also prioritize the communication of the firm's proactive measures and technologies deployed to mitigate cybersecurity risks.

In terms of control variables, the results offer additional insights into the dynamics of CSD. For instance, the coefficient for FSIZE is negative and significant in Model 1 (CSD), suggesting that larger firms may be more cautious in their disclosures, possibly due to concerns about revealing sensitive information. This aligns with the notion that larger firms have more to lose from detailed disclosures and might opt for a more guarded approach (Gao et al., 2020; Radu & Smaili, 2022). Conversely, the positive impact of intangible assets (INTAN) on all three CSD measures indicates that firms with significant intangible assets, such as intellectual property and digital resources, are more likely to disclose cybersecurity information, reflecting their vulnerability to cyber risks and their need to reassure stakeholders (Haislip et al., 2020; Hilary et al., 2016; Smaili et al., 2023).

Likewise, return on equity (ROE) has a significant positive effect on both CSD and CRMT, suggesting that more profitable firms tend to disclose more cybersecurity information. This could be because profitable firms have more resources to invest in cybersecurity measures and are keen to showcase these efforts to their stakeholders as part of their broader governance and

risk management strategies (Gull et al., 2018; Kamiya et al., 2021). Board size (BSIZE) is positively associated with all disclosure measures, reflecting the enhanced governance capacity of larger boards, which are better equipped to address complex issues like cybersecurity, as larger boards tend to have more diverse expertise and resources (Lanis & Richardson, 2011; Minichilli et al., 2009; Post & Byron, 2015). Lastly, board gender diversity (BGD) positively impacts overall CSD and CRMT, highlighting the role of female directors on boards in promoting transparency and effective governance. This finding is consistent with prior studies that emphasized the positive impact of gender diversity on board effectiveness and corporate transparency, suggesting that diverse boards are better equipped to understand and communicate complex issues like cybersecurity (Post & Byron, 2015; Radu & Smaili, 2022; Smaili et al., 2023; Wahid, 2019).

These results are consistent with prior studies (e.g., Amir et al., 2018; Haislip et al., 2020; Héroux & Fortin, 2022; Smaili et al., 2023), which indicated the significant positive influence of individual board governance mechanisms on corporate CSD. Furthermore, these findings are consistent with RDT, which posits that boards equipped with specialized expertise in IT and cybersecurity are better positioned to access and deploy critical resources that enhance a firm's strategic focus on cybersecurity (Mallin et al., 2013; Pfeffer & Salancik, 1978). Such boards can effectively oversee and promote comprehensive CSD, ensuring that the firm is both adequately prepared for and transparent about its cybersecurity risks.

In addition, the findings support stakeholder theory, emphasizing that organizations must address the concerns of a broad range of stakeholders, not just shareholders (Freeman, 2010; Radu & Smaili, 2022). The significant impact of BCCG on CSD indicates that firms with strong

BCCG are more likely to respond to stakeholder demands for greater transparency in this area. This result suggests that these firms are proactively acknowledging and addressing the broader concerns of stakeholders, including customers, regulators, and the public, who are increasingly attentive to cybersecurity risks and practices.

Overall, the results emphasize the crucial role of board commitment in shaping corporate disclosure in cybersecurity matters. Firms with a committed and capable board are more likely to engage in comprehensive CSD, thereby fulfilling both regulatory obligations and stakeholder expectations. This study underscores the importance of integrating strong cybersecurity governance practices at the board level to enhance the firm's overall disclosure practices, thereby boosting its reputation and legitimacy in an increasingly digital and risk-prone environment. These findings align with the study's expectations, providing empirical support for the first hypothesis, H1, that BCCG is positively associated with corporate CSD.

[Inset Table 5]

5.2.2. The direct and moderating effects of NIS regulation

Table 6 presents the results for the two hypotheses concerning the direct and moderating effects of the NIS Regulation (H2 and H3), reported in relation to the three models for each CSD proxy. The findings in Models 1-3 show that the NIS regulation has a statistically significant positive relationship with overall CSD ($\beta = 0.260$, $p < 0.01$), CSTI ($\beta = 0.110$, $p < 0.01$), and CRMT ($\beta = 0.392$, $p < 0.01$), suggesting that the introduction of the NIS regulation has significantly increased the extent of CSD by firms. These results are consistent with the predictions of institutional theory, which posits that firms conform to regulatory frameworks to gain legitimacy within their institutional environment (DiMaggio & Powell, 1983).

The positive impact of the NIS regulation on CSD indicates that firms are not only complying with regulatory demands but are also using these disclosures as a strategy to legitimize their cybersecurity practices and align with societal expectations (Héroux & Fortin, 2022; North, 1990). This is largely in line with prior research that suggests adherence to regulations might help firms to legitimize management decisions and actions (e.g., Hombach & Sellhorn, 2019; Hummel & Rötzel, 2019; Rogerson et al., 2020; Thielemann et al., 2019). This evidence is also consistent with stakeholder theory, which suggests that firms are motivated to increase transparency in response to growing scrutiny from various stakeholders (Freeman, 2010; Walton et al., 2021). The positive relationship between NIS and CSD supports the notion that firms, even those not directly mandated by NIS, are driven to enhance their disclosure practices to maintain legitimacy and meet the informational needs of their stakeholders (Rogerson et al., 2020). These findings provide empirical support for H2, suggesting that the NIS regulation positively influences CSD.

In terms of the moderating effect hypothesized in H3, the interaction term between BCCG and NIS shows a positive and significant relationship with overall CSD in Model 1 of Table 6 ($\beta = 0.278$, $p < 0.05$) and CRMT in Model 3 ($\beta = 0.613$, $p < 0.01$). These results suggest that the NIS regulation enhances the positive relationship between BCCG and CSD, particularly in the areas of overall disclosures and risk mitigation strategies. This aligns with institutional theory, which posits that regulations like the NIS act as external catalysts, compelling firms to align their practices with established norms and rules to gain legitimacy (DiMaggio & Powell, 1983). The NIS regulation enhances the impact of BCCG by providing a regulatory framework that reinforces the importance of cybersecurity governance and encourages firms to disclose more detailed and comprehensive information. This strategic alignment with regulatory

expectations fulfils compliance requirements and strengthens the firm's standing within its institutional context (North, 1990).

Moreover, this moderating effect is consistent with the principles of stakeholder theory, which suggests that firms are motivated to address the diverse informational needs of their stakeholders through enhanced disclosure practices (Freeman, 2010). The positive impact of BCCG on CSD, particularly when amplified by NIS, reflects a firm's broader commitment to transparency and accountability, which are critical for building trust and confidence among stakeholders (Cooper & Slack, 2015; Talbot & Boiral, 2018). This finding underscores the importance of regulatory frameworks in shaping corporate behavior, particularly in areas like CSD, where stakeholder expectations are high.

However, the non-significant interaction effect between BCCG and NIS in Model 2 (CSTI) suggests that the disclosure of cybersecurity threats and incidents may be less influenced by external regulatory pressures and more dependent on the intrinsic commitment of the board to transparency. This could be attributed to the sensitive nature of such disclosures, where firms might prioritize competitive concerns or reputational risks over regulatory incentives, even with a committed board. This is consistent with the findings of Amir et al. (2018), who noted that firms with weaker governance structures tend to withhold information on cyber-attacks, indicating that the board's intrinsic motivation is crucial in deciding the extent of such disclosures.

In summary, we conclude that our argument is supported by empirical evidence, leading us to accept H2 and H3. Specifically, the NIS regulation positively influences CSD (H2) and

moderates the relationship between BCCG and disclosure practices, particularly in the area of risk mitigation (H3). These results highlight the complementary roles of internal governance and external regulatory frameworks in shaping corporate disclosure practices in the cybersecurity domain.

[Insert Table 6]

6. Additional analyses and robustness checks

6.1. Testing subsamples based on corporate governance, firm size and profitability

Table 7 presents a detailed analysis of subsamples based on the strength of corporate governance, firm size, and profitability to deepen our understanding of how these factors influence the relationship between BCCG and CSD.

First, we re-estimate our main specification by splitting the sample into two subsamples based on the strength of firms' corporate governance: (i) strong governance (composite governance score above the industry median) and (ii) weak governance (composite governance score below the industry median). The results in Table 7 (Models 1 and 2) reveal that BCCG significantly influences CSD across firms, regardless of governance strength. Interestingly, the influence is stronger in firms with weaker governance (Model 2). This suggests that firms with weaker governance may be more motivated to enhance their CSD to compensate for broader governance deficiencies. By being more transparent about cybersecurity practices, these firms can build trust and credibility among stakeholders. This approach aligns with RDT (Pfeffer & Salancik, 1978), which posits that organizations rely on their board's expertise to manage external dependencies and risks. Weaker governance firms might use CSD as a strategic tool to signal their commitment to managing specific risks, like cybersecurity, to mitigate concerns

and enhance their reputation. This contrasts with Amir et al. (2018), who found that firms with stronger governance are more likely to disclose information due to established fiduciary responsibilities. In conclusion, our findings indicate that BCCG has a significant positive impact on CSD, with this influence being more pronounced in firms with weaker governance.

Second, we repeat the main analysis by splitting the sample based on firm size, distinguishing between (i) large firms, where firm size is above the industry median, and (ii) small firms, where firm size is below the industry median. The results are presented in Table 7. Models 3 and 4 reveal a positive and significant association between BCCG and CSD across both firm sizes. This result suggests that increased BCCG is consistently related to higher levels of CSD (Carter & Lorsch, 2003; Haislip et al., 2020; Radu & Smaili, 2022). Particularly, the relationship is more pronounced in smaller firms (Model 4), indicating that these firms may place greater emphasis on CSD as a means to build trust and credibility with stakeholders. This heightened commitment among smaller firms may be driven by their need to align with societal values and norms (stakeholder theory) and adhere to governmental guidelines (institutional theory). Smaller firms may view CSD as a strategic means to respond to institutional pressures and demonstrate compliance with cybersecurity regulations and industry best practices (DiMaggio & Powell, 1983).

Lastly, we divided our sample based on firms' financial performance into two subsamples: (i) high-performing firms and (ii) low-performing firms. The results are presented in Table 7. Model 5 captures the effects of BCCG on CSD for high-performing firms, while Model 6 does the same for low-performing firms. Our findings indicate that BCCG significantly influences CSD across both subsamples, but the impact is more pronounced in high-performing firms.

This suggests that firms with higher profitability are better equipped to invest in comprehensive cybersecurity practices; this is likely due to their greater access to resources. Consequently, these firms may leverage CSD as a strategic tool to address stakeholder concerns – aligning with stakeholder theory – and to enhance corporate legitimacy and reputation – which is consistent with institutional theory. Therefore, high-performing firms may view enhanced CSD as an opportunity to further strengthen their stakeholder relationships and to position themselves as industry leaders in governance and transparency (Gull et al., 2018; Kamiya et al., 2021).

To summarize, the findings in this section offer further evidence of the significant role that BCCG plays in shaping CSD across various subsamples. The consistent impact of BCCG, regardless of governance strength, firm size, or profitability, underscores its importance as a key factor in driving disclosure practices.

[Insert Table 7]

6.2. Alternative measures of CSD and BCCG

To ensure the robustness of our findings, we first explore alternative measures for the CSD and BCCG compared to our main Models. To examine whether our results are sensitive to the CSD proxy employed, we replicate our results in Table 6 by replacing our sentence count CSD measure with the firm's propensity to disclose cybersecurity information. We construct a dummy variable, assigning 1 if the firm discloses cybersecurity information and 0 otherwise. Using logistic regression, the results in Panel A, Models 1-3 of Table 8 support our previous findings regarding the influence of BCCG and NIS on CSD, CSTI, and CRMT (Ben-Amar & McIlkenny, 2015; Smaili et al., 2023). In addition, following prior research (e.g., Campbell, 2004; Loughran & McDonald, 2011; Smaili et al., 2023), we further validated our results by

replacing our sentence count CSD measure with a word count CSD measure. These results (un-tabulated) are generally consistent with those in Table 6, suggesting that our evidence is robust across alternative measures for CSD.

Second, following Albitar et al. (2023), we computed an alternative measure of BCCG by aggregating five cybersecurity and IT-related board attributes. This new measure, scaled from 0 to 5, allowed for a quantifiable evaluation of the board-level commitment to cybersecurity risks. This scaling simplifies the interpretation of the board's commitment to cybersecurity, making it more accessible for comparative analysis. The results reported in Panel B, Models 1-3 of Table 8, are primarily compatible with the main analysis; the impact of BCCG and NIS variables on CSD, CSTI, and CRMT remains consistent.

[Insert Table 8]

6.3. Lagged CSD–BCCG Relationships

To address potential endogeneity issues where CSD and BCCG might be simultaneously determined, we estimated a lagged CSD–BCCG structure (Larcker & Rusticus, 2010). We re-ran our main model, incorporating a one-year lag between CSD and BCCG. The results, presented in Panel C, Models 1-3 of Table 8, consistently support our main findings, reinforcing the robustness of the positive relationship between BCCG and CSD, even after accounting for potential reverse causality. Specifically, the lagged model continues to demonstrate significant positive effects of BCCG on subsequent CSD, both in aggregate (CSD) and across specific categories (CSTI and CRMT). This temporal sequencing strengthens our argument that BCCG is a driving force behind enhanced disclosure practices.

6.4. 2SLS, 3SLS, and Heckman Two-Stage Models

To address potential endogeneity concerns, we employed 2SLS and 3SLS instrumental variable regression approaches. These methods are particularly effective for estimating simultaneous equation models in dynamic random effects contexts (Trinh et al., 2024; Zellner & Theil, 1992). The 3SLS approach, in particular, may offer greater efficiency than 2SLS as it accounts for cross-equation correlations and does not impose restrictions on the auto covariance matrix of errors, thereby avoiding the assumption of normally distributed errors (Zellner & Theil, 1992).

In line with the instrumenting technique used in prior literature (e.g., Anginer et al., 2014; Safiullah & Shamsuddin, 2019; Trinh et al., 2024), we selected our instrumental variables (IVs) to include the year-average of BCCG characteristics (excluding dummy variables) from other firms in the same year within our sample. This instrumental variable is appropriate for two reasons: (i) it is likely to correlate with the BCCG of the observed firm, as firms within the same year and industry tend to follow their peers in governance practices, and (ii) changes in one firm's level of cybersecurity-related disclosure are unlikely to be associated with the BCCG characteristics of other firms. The IV regression results, presented in Models 1& 2 of Table 9, show that BCCG is positively significant with CSD in both the 2SLS and 3SLS models. Additionally, the test of endogeneity confirms the appropriateness of using the instrumental variable approach (p-value = 0.000), and the first-stage F-tests confirm the strength of the instruments (p-value = 0.000). The Breusch-Pagan LM test for heteroscedasticity also indicates the presence of heteroscedasticity (p-value = 0.000). These findings reinforce the robustness of our results, confirming that BCCG significantly enhances the level of CSD.

Furthermore, to address potential sample selection bias, we conducted a Heckman two-stage analysis, consistent with prior literature (De Franco et al., 2013; Hoelscher, 2020; Wang et al., 2020). In the first stage, a probit model was used to predict the probability of firms disclosing cybersecurity information, from which the inverse Mills ratio was calculated. In the second stage, we included the inverse Mills ratio in the regression of CSD scores on BCCG, along with other control variables. The results from the second stage, presented in Model 4 of Table 9, show that BCCG remains positively and significantly associated with CSD (coefficient = 2.254, $p < 0.01$), consistent with our main findings.

[Insert Table 9]

6.5. Difference-in-Differences (DiD) analysis

To more effectively tackle the endogeneity issues related to the influence of NIS regulation on CSD, we followed previous studies (Balakrishnan et al., 2019; Chen et al., 2018; Downar et al., 2021; Nguyen, 2021) by utilizing the NIS regulation as a quasi-natural experiment in our DiD analysis. We analyzed the differences between pre- and post-NIS cybersecurity data for affected firms, comparing them with cybersecurity data from a control group of firms over a seven-year period surrounding the year 2018. The treatment group in our DiD analysis consists of firms in industries that were subject to the NIS regulation (NIS, 2018), namely, energy, transport, water, and healthcare, and digital infrastructure. These firms are expected to have adopted or improved cybersecurity measures to comply with the new regulations. The control group comprises firms from other industries not identified under the NIS regulation. These firms serve as a baseline to measure changes in the treatment group, under the assumption they have not experienced the same regulatory pressures.

To further control inherent differences between the treated and control groups prior to the NIS event, we employed the PSM technique to pair similar firms. Initially, we conducted a logit regression of the treatment dummy on all control variables as indicated in Table 5, estimating the probability of a firm being in the treatment group, using our pre-NIS regulation data. Subsequently, we match each treatment firm with a control firm using the nearest neighbor matching technique (within a 0.01 caliper) without replacement (Dehejia & Wahba, 2002). This approach yields a primary PSM sample of 1063 firm-years, comprising 417 treatment firm-years and 646 control firm-years. The pre-match diagnostic test (Panel A of Table 10) shows significant initial differences between treated and control groups in variables such as firm size, intangible assets, and leverage, emphasizing the distinct characteristics of firms subject to NIS regulations. Post-match diagnostic results (Panel B of Table 10) reveal no significant differences in all control characteristics between the treatment and control groups, thus confirming that the two groups are comparable for our analysis after matching.

We estimate the following DiD regression model using the PSM-matched sample to explore the impact of NIS regulation on CSD. The model regresses CSD on a dummy variable (*Post*) indicating the post-NIS period (2018-2021), a dummy variable (*Treatment*) indicating if the firm is subject to NIS regulation, and their interaction term. Specifically, our DiD regression model is as follows:

$$CSD_{it} = \alpha_0 + \beta_1 Post_{it} + \beta_2 Treatment_{it} + \beta_3 Post_{it} * Treatment_{it} + \sum_{i=1}^n \beta_i CONTROLS_{it} + \varepsilon_{it} \quad (3)$$

where:

Post_{it}: A dummy variable that equals 1 if the observation is from the post-NIS period (2018-2021), and 0 otherwise. This captures the time effect of the regulation on all firms.

Treatment_{it}: A dummy variable that equals 1 if the firm is in an industry affected by the NIS regulation (treatment group), and 0 if it is in the control group. This captures the effect of being under the NIS regulatory umbrella.

*Post_{it} * Treatment_{it}*: Interaction term between the post-NIS period and treatment group. The coefficient β_3 measures the differential impact of the NIS regulation on the cybersecurity disclosure of treated firms relative to control firms, hence capturing the causal effect of the NIS directive. A negative (positive) β_3 implies a decrease (increase) in CSD post-NIS regulation.

The results, as shown in Panel C of Table 10, reveal a significant positive coefficient on Post for CSD. This indicates an increase in CSD for control firms after the NIS introduction. Furthermore, the coefficient on Treatment firms is also significantly positive, suggesting that treatment firms have higher CSD compared to control firms before the NIS implementation. Importantly, the estimated coefficient on the interaction term, $\text{Post} \times \text{Treatment}$, is significantly positive, indicating that treatment firms experience an increased CSD compared to control firms post-NIS regulation. These results suggest that firms are responding to NIS regulation with heightened levels of CSD.

[Insert Table 10]

7. Conclusion

This study provides a comprehensive analysis of board commitment to cybersecurity governance and its impact on cybersecurity disclosure, with a specific focus on the moderating role of the UK NIS regulation. Utilizing a robust dataset from FTSE 350 firms over the period 2015–2021, we developed a composite measure to assess the level of CSD and BCCG. Our findings indicate a positive correlation between BCCG and the extent of CSD. Particularly noteworthy is the finding that boards with substantial IT expertise and established cybersecurity policies and committees are more proactive in their disclosure practices,

especially in areas such as cybersecurity risk mitigation and technologies. This relationship is further strengthened in the presence of the NIS regulation.

From a theoretical perspective, our research supports and extends the principles of resource dependence, stakeholder, and institutional theories. The study underscores the significant role of board composition, particularly IT expertise, in shaping cybersecurity governance and disclosure practices. Furthermore, it highlights the importance of considering broader stakeholder needs and expectations in the realm of cybersecurity, beyond just shareholder interests. The findings also emphasize the influential role of regulatory frameworks, such as the NIS, in guiding corporate conduct towards increased disclosure in cybersecurity. The findings can encourage cross-disciplinary research between cybersecurity, corporate governance, and sustainable development. This can lead to a more holistic approach to understanding and achieving resilient and innovative infrastructure as part of SDG 9.

In practical terms, our study unveils profound implications for policymakers, managers, and stakeholders. Aligned with the United Nations' Sustainable Development Goal 9 (SDG 9), which underscores the necessity of building resilient infrastructure and fostering innovation, our findings highlight the pivotal role of corporate governance in cybersecurity. The study illuminates the critical role that a robust commitment to cybersecurity within corporate boards, characterized by specific IT expertise and proactive governance mechanisms, plays in enhancing transparency around cybersecurity practices.

The demonstrated positive association between BCCG and the levels of CSD articulates a clear cause-effect relationship that has multiple layers of implications. For one, it suggests that

firms with a strong governance framework are more transparent in their cybersecurity practices, thereby potentially reducing the risk premium associated with cyber vulnerabilities. This transparency can lead to enhanced investor confidence and could serve as a buffer against market volatility stemming from cybersecurity incidents. Indeed, this can be examined in future research. Furthermore, these insights can inform the refinement of regulatory frameworks, ensuring they more effectively mandate and reinforce the need for comprehensive CSD.

In addition, policymakers are thus encouraged to consider these findings in the ongoing enhancement of regulations like the NIS. Enhancements could include stipulations for greater specificity in CSD and requirements for board members' cybersecurity competencies. Such regulatory adjustments would not only elevate the standard of cybersecurity practices across industries, but they would also improve compliance and accountability, enhancing the overall cyber resilience of the economic landscape.

Additionally, the findings advocate for the adoption and enforcement of governance codes that emphasize the importance of IT expertise on corporate boards, the establishment of dedicated IT committees, and the implementation of comprehensive cybersecurity policies. By integrating these elements, firms can significantly elevate their cybersecurity posture and response capabilities, which is indispensable in today's rapidly evolving threat environment. Reflecting the increasing importance of cybersecurity in corporate governance, these measures could serve as benchmarks for best practices, guiding firms in various sectors toward safer and more resilient digital operations. Ultimately, this study confirms the critical role of effective board governance in cybersecurity and provides a clear roadmap for enhancing corporate and regulatory practices that could lead to a more secure global digital economy.

This study, however, has some limitations and avenues for future research. Firstly, while our focus on UK FTSE350 firms provides valuable insights, further research could replicate our study in other countries with different institutional and cultural contexts. Secondly, a notable limitation concerns the potential use of boilerplate language in annual reports. As identified in prior research (e.g., Li et al., 2018), there is a possibility that firms may include standardized, non-substantive cybersecurity-risk information in their disclosures. This practice can result from firms following general disclosure guidance without necessarily reflecting material cybersecurity risks.

To mitigate this issue, our study employed a rigorous keyword-based analysis combined with manual verification to ensure the relevance and specificity of the cybersecurity information extracted from annual reports. Despite these efforts, the inherent nature of textual analysis means that some disclosures identified might still represent boilerplate content that does not provide meaningful insight into the firm's actual cybersecurity posture.

Thirdly, our study primarily employs quantitative methods; future research could benefit from incorporating qualitative approaches, such as interviews with board members or cybersecurity experts. These could provide deeper insights into the decision-making processes behind cybersecurity governance and disclosure. Finally, future research could also examine the impact of corporate board leadership features on CSD, such as CEO power and business strategy.

Data availability statement:

The article makes use of existing (secondary) data.

References

- Albitar, K., Al-Shaer, H., & Liu, Y. S. (2023). Corporate commitment to climate change: The effect of eco-innovation and climate governance. *Research Policy*, 52(2), 104697. <https://doi.org/10.1016/j.respol.2022.104697>
- Allam, A., Moussa, T., & Elmarzouky, M. (2024). Examining the relationship between CEO power and modern slavery disclosures: The moderating role of board gender diversity in UK companies. *Business Strategy and the Environment*, 33(8), 8067–8085. <https://doi.org/10.1002/bse.3910>
- 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>
- Anginer, D., Demircuc-Kunt, A., & Zhu, M. (2014). How does competition affect bank systemic risk? *Journal of Financial Intermediation*, 23(1), 1–26.
- Arena, C., Bozzolan, S., & Michelon, G. (2015). Environmental reporting: Transparency to stakeholders or stakeholder manipulation? An analysis of disclosure tone and the role of the board of directors. *Corporate Social Responsibility and Environmental Management*, 22(6), 346–361. <https://doi.org/10.1002/csr.1350>
- Balakrishnan, K., Blouin, J. L., & Guay, W. R. (2019). Tax aggressiveness and corporate transparency. *The Accounting Review*, 94(1), 45–69. <https://doi.org/10.2308/accr-52130>
- Ben-Amar, W., & Belgacem, I. (2018). Do socially responsible firms provide more readable disclosures in annual reports? *Corporate Social Responsibility and Environmental Management*, 25(5), 1009–1018. <https://doi.org/10.1002/csr.1517>
- Ben-Amar, W., & McIlkenny, P. (2015). Board effectiveness and the voluntary disclosure of climate change information. *Business Strategy and the Environment*, 24(8), 704–719. <https://doi.org/10.1002/bse.1840>
- Birkey, R. N., Guidry, R. P., Islam, M. A., & Patten, D. M. (2018). Mandated social disclosure: An analysis of the response to the California Transparency in Supply Chains Act of 2010. *Journal of Business Ethics*, 152(3), 827–841. <https://doi.org/10.1007/s10551-016-3364-7>
- Bravo, F., & Alcaide-Ruiz, M. D. (2019). The disclosure of financial forward-looking information: Does the financial expertise of female directors make a difference? *Gender in Management: An International Journal*, 34(2), 140–156. <https://doi.org/10.1108/GM-09-2018-0120>
- BT Group. (2018). *Annual reports—Financial reporting & news—Investors | BT Plc.* <https://www.bt.com/about/investors/financial-reporting-and-news/annual-reports>
- Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, 25(1), 24–39. <https://doi.org/10.1111/ijau.12209>
- 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, D. (2004). A longitudinal and cross-sectional analysis of environmental disclosure in UK companies—A research note. *The British Accounting Review*, 36(1), 107–117.
- Carter, C. B., & Lorsch, J. W. (2003). *Back to the drawing board: Designing corporate boards for a complex world*. Harvard Business Press.

- 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, Y. C., Hung, M., & Wang, Y. (2018). The effect of mandatory CSR disclosure on firm profitability and social externalities: Evidence from China. *Journal of Accounting and Economics*, 65(1), 169–190. <https://doi.org/10.1016/j.jacceco.2017.11.009>
- Cohen, J. (1960). A Coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1), 37–46. <https://doi.org/10.1177/001316446002000104>
- Collis, J., & Hussey, R. (2021). *Business research: A practical guide for students*. Bloomsbury Publishing.
- Cooper, S., & Slack, R. (2015). Reporting practice, impression management and company performance: A longitudinal and comparative analysis of water leakage disclosure. *Accounting and Business Research*, 45(6–7), 801–840. <https://doi.org/10.1080/00014788.2015.1081554>
- De Franco, G., Hope, O.-K., & Larocque, S. (2013). The effect of disclosure on the pay-performance relation. *Journal of Accounting and Public Policy*, 32(5), 319–341.
- Dehejia, R. H., & Wahba, S. (2002). Propensity score-matching methods for nonexperimental causal studies. *The Review of Economics and Statistics*, 84(1), 151–161. <https://doi.org/10.1162/003465302317331982>
- Desender, K. A., Aguilera, R. V., Lópezpuertas-Lamy, M., & Crespi, R. (2016). A clash of governance logics: Foreign ownership and board monitoring. *Strategic Management Journal*, 37(2), 349–369. <https://doi.org/10.1002/smj.2344>
- 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>
- Downar, B., Ernstberger, J., Reichelstein, S., Schwenen, S., & Zaklan, A. (2021). The impact of carbon disclosure mandates on emissions and financial operating performance. *Review of Accounting Studies*, 26(3), 1137–1175. <https://doi.org/10.1007/s11142-021-09611-x>
- Elamer, A. A., Ntim, C. G., & Abdou, H. A. (2020). Islamic governance, national governance, and bank risk management and disclosure in MENA countries. *Business & Society*, 59(5), 914–955. <https://doi.org/10.1177/0007650317746108>
- Elnahass, M., Ahmed, Y., & Trinh, V. Q. (2024). Empowering women to lead cybersecurity: The effect of female executives on disclosure sentiment. *International Journal of Finance & Economics*, n/a(n/a). <https://doi.org/10.1002/ijfe.3067>
- Fernando, S., & Lawrence, S. (2014). A theoretical framework for CSR practices: Integrating legitimacy theory, stakeholder theory, and institutional theory. *The Journal of Theoretical Accounting Research*, 10(1), 149–178.
- 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>
- Freeman, E. (2010). *Strategic management: A stakeholder approach*. Cambridge University Press.
- Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 38, 100468. <https://doi.org/10.1016/j.accinf.2020.100468>
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 567–594.

- Gull, A. A., Nekhili, M., Nagati, H., & Chtioui, T. (2018). Beyond gender diversity: How specific attributes of female directors affect earnings management. *The British Accounting Review*, 50(3), 255–274. <https://doi.org/10.1016/j.bar.2017.09.001>
- Haislip, J. Z., Karim, K. E., Lin, K. J., & Pinsker, R. E. (2020). The Influences of CEO IT Expertise and Board-Level Technology Committees on Form 8-K Disclosure Timeliness. *Journal of Information Systems*, 34(2), 167–185. <https://doi.org/10.2308/isisys-52530>
- Hasseldine, J., Salama, A. I., & Toms, J. S. (2005). Quantity versus quality: The impact of environmental disclosures on the reputations of UK Plcs. *The British Accounting Review*, 37(2), 231–248. <https://doi.org/10.1016/j.bar.2004.10.003>
- Helfaya, A., & Moussa, T. (2017). Do board's corporate social responsibility strategy and orientation influence environmental sustainability disclosure? UK evidence. *Business Strategy and the Environment*, 26(8), 1061–1077.
- Helfaya, A., & Whittington, M. (2019). Does designing environmental sustainability disclosure quality measures make a difference? *Business Strategy and the Environment*, 28(4), 525–541. <https://doi.org/10.1002/bse.2262>
- Héroux, S., & Fortin, A. (2022). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance*. <https://doi.org/10.1007/s10997-022-09660-7>
- Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, 30(3), 79–98. <https://doi.org/10.2308/isisys-51402>
- Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: Who cares? *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2852519>
- Hoelscher, S. A. (2020). Voluntary hedging disclosure and corporate governance. *Review of Accounting and Finance*, 19(1), 5–29.
- Hombach, K., & Sellhorn, T. (2019). Shaping corporate actions through targeted transparency regulation: A framework and review of extant evidence. *Schmalenbach Business Review*, 71(2), 137–168. <https://doi.org/10.1007/s41464-018-0065-z>
- Hummel, K., & Rötzel, P. (2019). Mandating the sustainability disclosure in annual reports—Evidence from the United Kingdom. *Schmalenbach Business Review*, 71(2), 205–247. <https://doi.org/10.1007/s41464-019-00069-8>
- IBM. (2024). *Cost of a data breach 2024*. <https://www.ibm.com/reports/data-breach>
- Jain, T., & Zaman, R. (2020). When boards matter: The case of corporate social irresponsibility. *British Journal of Management*, 31(2), 365–386. <https://doi.org/10.1111/1467-8551.12376>
- 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>
- Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th.). Sage publications.
- Lanis, R., & Richardson, G. (2011). The effect of board of director composition on corporate tax aggressiveness. *Journal of Accounting and Public Policy*, 30(1), 50–70. <https://doi.org/10.1016/j.jaccpubpol.2010.09.003>
- Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems*, 35(1), 101–119. <https://doi.org/10.2308/isisys-18-071>

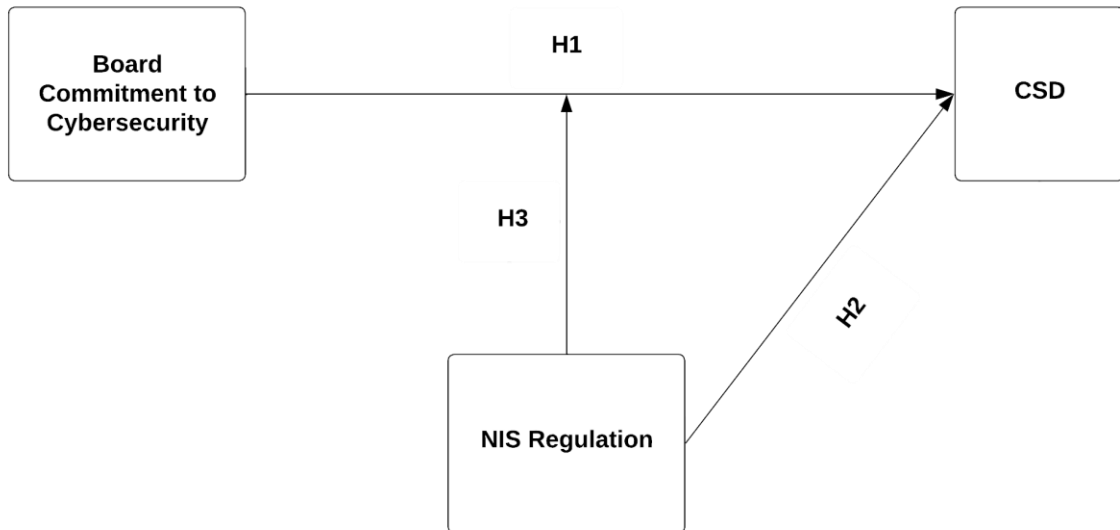
- Larcker, D. F., & Rusticus, T. O. (2010). On the use of instrumental variables in accounting research. *Journal of Accounting and Economics*, 49(3), 186–205. <https://doi.org/10.1016/j.jacceco.2009.11.004>
- Lattanzio, G., & Ma, Y. (2023). Cybersecurity risk and corporate innovation. *Journal of Corporate Finance*, 82, 102445. <https://doi.org/10.1016/j.jcorpfin.2023.102445>
- 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, Y., Gong, M., Zhang, X.-Y., & Koh, L. (2018). The impact of environmental, social, and governance disclosure on firm value: The role of CEO power. *The British Accounting Review*, 50(1), 60–75. <https://doi.org/10.1016/j.bar.2017.09.007>
- 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>
- Mallin, C. A., & Michelon, G. (2011). Board reputation attributes and corporate social performance: An empirical investigation of the US best corporate citizens. *Accounting and Business Research*, 41(2), 119–144.
- Mallin, C. A., Michelon, G., & Raggi, D. (2013). Monitoring intensity and stakeholders' orientation: How does governance affect social and environmental disclosure? *Journal of Business Ethics*, 114(1), 29–43.
- Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 105336. <https://doi.org/10.1016/j.clsr.2019.06.007>
- Marquardt, D. W. (1970). Generalized inverses, ridge regression, biased linear estimation, and nonlinear estimation. *Technometrics*, 12(3), 591–612. <https://doi.org/10.2307/1267205>
- Marshall Plc. (2021). *Annual & Interim Reports | Presentations & Speeches | Marshalls*. <https://www.marshalls.co.uk/investor/results-reports-and-presentations>
- Masud, M. A. K., Bae, S. M., Manzanares, J., & Kim, J. D. (2019). Board directors' expertise and corporate corruption disclosure: The moderating role of political connections. *Sustainability*, 11(16), 4491. <https://doi.org/10.3390/su11164491>
- McIntyre, M. L., Murphy, S. A., & Mitchell, P. (2007). The top team: Examining board composition and firm performance. *Corporate Governance*, 7(5), 547. <https://doi.org/10.1108/14720700710827149>
- Minichilli, A., Zattoni, A., & Zona, F. (2009). Making boards effective: An empirical examination of board task performance. *British Journal of Management*, 20(1), 55–74. <https://doi.org/10.1111/j.1467-8551.2008.00591.x>
- Moussa, T., Allam, A., & Elmarzouky, M. (2023). An examination of UK companies' modern slavery disclosure practices: Does board gender diversity matter? *Business Strategy and the Environment*, 32(8). <https://doi.org/10.1002/bse.3426>
- Naheed, R., AlHares, A., Shahab, Y., & Naheed, R. (2021). Board's financial expertise and corporate social responsibility disclosure in China. *Corporate Governance*, 21(4), 716–736. <https://doi.org/10.1108/CG-08-2020-0329>
- Nguyen, J. H. (2021). Tax avoidance and financial statement readability. *European Accounting Review*, 30(5), 1043–1066. <https://doi.org/10.1080/09638180.2020.1811745>
- NIS. (2018). *The Network and Information Systems Regulations 2018*. King's Printer of Acts of Parliament. <https://www.legislation.gov.uk/ukxi/2018/506/contents/made>

- North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge university press.
- Pae, J., & Choi, T. H. (2011). Corporate governance, commitment to business ethics, and firm valuation: Evidence from the Korean stock market. *Journal of Business Ethics*, 100(2), 323–348. <https://doi.org/10.1007/s10551-010-0682-z>
- Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper and Row.
- Post, C., & Byron, K. (2015). Women on boards and firm financial performance: A meta-analysis. *Academy of Management Journal*, 58(5), 1546–1571. <https://doi.org/10.5465/amj.2013.0319>
- Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics*, 177, 1–24. <https://doi.org/10.1007/s10551-020-04717-9>
- Rogerson, M., Crane, A., Soundararajan, V., Grosvold, J., & Cho, C. H. (2020). Organisational responses to mandatory modern slavery disclosure legislation: A failure of experimentalist governance? *Accounting, Auditing & Accountability Journal*, 33(7), 1505–1534. <https://doi.org/10.1108/AAAJ-12-2019-4297>
- Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: Evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, 54(03), 1950013. <https://doi.org/10.1142/S1094406019500136>
- Safiullah, M., & Shamsuddin, A. (2019). Risk-adjusted efficiency and corporate governance: Evidence from Islamic and conventional banks. *Journal of Corporate Finance*, 55, 105–140.
- Salin, A. S. A. P., Ismail, Z., Smith, M., & Nawawi, A. (2019). The influence of a board's ethical commitment on corporate governance in enhancing a company's corporate performance. *Journal of Financial Crime*, 26(2), 496–518. <https://doi.org/10.1108/JFC-04-2018-0035>
- Shahab, Y., Ntim, C. G., Chen, Y., Ullah, F., Li, H.-X., & Ye, Z. (2020). Chief executive officer attributes, sustainable performance, environmental performance, and environmental reporting: New insights from upper echelons perspective. *Business Strategy and the Environment*, 29(1), 1–16. <https://doi.org/10.1002/bse.2345>
- Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, 27(4), 1049–1071. <https://doi.org/10.1007/s10997-022-09637-6>
- Talbot, D., & Boiral, O. (2018). GHG reporting and impression management: An assessment of sustainability reports from the energy sector. *Journal of Business Ethics*, 147(2), 367–383. <https://doi.org/10.1007/s10551-015-2979-4>
- Thielemann, F., Dinh, T., & Kang, H. (2019). Non-GAAP reporting and debt market outcomes: Evidence from Regulation G. *Schmalenbach Business Review*, 71(2), 169–203. <https://doi.org/10.1007/s41464-019-00074-x>
- Trinh, V. Q., Elnahass, M., & Pasiouras, F. (2024). Personal traits of CEOs and cybersecurity-related disclosure. *Journal of International Accounting, Auditing and Taxation*, Forthcoming. <https://doi.org/10.2139/ssrn.4782601>
- Tunyi, A. A., & Ntim, C. G. (2016). Location advantages, governance quality, stock market development, and firm characteristics as antecedents of African M&As. *Journal of International Management*, 22(2), 147–167. <https://doi.org/10.1016/j.intman.2016.01.005>

- Wahid, A. S. (2019). The effects and the mechanisms of board gender diversity: Evidence from financial manipulation. *Journal of Business Ethics*, 159(3), 705–725. <https://doi.org/10.1007/s10551-018-3785-6>
- Walton, S., Wheeler, P. R., Zhang, Y. (Ian), & Zhao, X. (Ray). (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, 35(1), 155–186. <https://doi.org/10.2308/ISYS-19-033>
- Wang, F., Xu, L., Guo, F., & Zhang, J. (2020). Loan guarantees, corporate social responsibility disclosure and audit fees: Evidence from China. *Journal of Business Ethics*, 166, 293–309.
- Wang, J., & Dewhirst, H. D. (1992). Boards of directors and stakeholder orientation. *Journal of Business Ethics*, 11(2), 115–123.
- Wilkin, C. L., & Chenhall, R. H. (2020). Information technology governance: Reflections on the past and future directions. *Journal of Information Systems*, 34(2), 257–292. <https://doi.org/10.2308/isys-52632>
- Wooldridge, J. M. (2010). *Econometric analysis of cross section and panel data*. MIT press.
- Zellner, A., & Theil, H. (1992). Three-stage least squares: Simultaneous estimation of simultaneous equations. In B. Raj & J. Koerts (Eds.), *Henri Theil's Contributions to Economics and Econometrics* (Vol. 23, pp. 147–178). Springer Netherlands. https://doi.org/10.1007/978-94-011-2546-8_10
- Zhang, Y. (2024). Data breach disclosure laws and social responsibility initiatives. *The International Journal of Accounting*. <https://doi.org/10.1142/S1094406024400031>

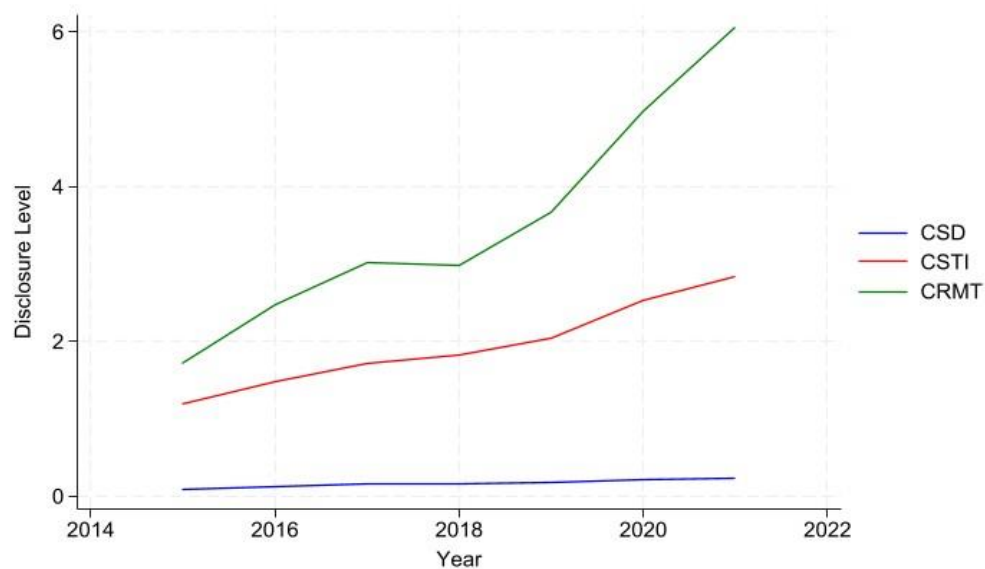
Figures

Figure 1: Research model



Note: This figure displays the hypothesized relationships between Board Commitment to Cybersecurity, NIS Regulation, and Cybersecurity Disclosures (CSD).

Figure 2: Trends of CSD, CSTI, and CRMT by year



Note: The figure illustrates the trends in Corporate Cybersecurity Disclosures (CSD), Cybersecurity Threats and Incidents (CSTI), and Cybersecurity Risk Mitigation and Technologies (CRMT) from 2015 to 2021

Tables

Table 1: Sample selection and distribution by industry

	Observations
Initial sample UK FTSE 350 firms	2450
Less:	
Obs. with missing annual reports	(210)
Obs. with missing data for required variables	<u>(363)</u>
Final sample	1877
Industry	Firm-year obs. (%)
Energy	52 (3%)
Basic Materials	91 (5%)
Industrials	335 (18%)
Consumer Discretionary	276 (15%)
Health Care	71 (4%)
Consumer Staples	124 (7%)
Telecommunications	38 (2%)
Utilities	46 (2%)
Real Estate	127 (7%)
Financials	668 (36%)
Technology	<u>49 (3%)</u>
Total	1877 (100%)

Note: This table presents the sample selection process and the distribution of firm-year observations by industry for the UK FTSE 350 firms included in the study.

Table 2: Descriptive statistics for all variables

Variable	Mean	Standard Deviation	Minimum	Maximum
CSD (%)	0.171	0.191	0.000	3.256
CSD (Number of sentences)	8.998	11.354	0.000	144.000
CSTI (%)	0.037	0.062	0.000	0.690
CRMT (%)	0.068	0.094	0.000	1.895
BITC	0.594	0.491	0.000	1.000
FCSP	0.321	0.467	0.000	1.000
BITEXP (%)	15.709	17.537	0.000	71.429
BDITEXP (%)	6.153	9.196	0.000	36.364
BINDITEXP (%)	6.079	10.567	0.000	42.857
BCCG	0.00	1.559	-1.628	5.767
FSIZE	14.837	1.779	11.410	20.505
INTAN	16.109	21.589	0.000	84.096
LEV	67.711	111.754	-207.280	613.220
MTBV	3.562	39.651	-1235.610	822.200
ROE	15.050	22.974	-64.420	119.180
LOSS	0.862	0.345	0.000	1.000
BSIZE	8.333	2.557	4.000	15.000
GOVS	58.366	23.620	0.890	98.560
BINDE	68.601	17.039	30.770	100.000
BGD	29.383	11.796	0.000	60.000

Notes: This table presents descriptive statistics of all variables used in our main analysis. CSD: Corporate cybersecurity disclosures, CSTI: Cybersecurity threats and incidents, CRMT: Cybersecurity risk mitigation and technologies, FCSP: Cybersecurity policy, BITC: Board IT committee, BITEXP: Board IT expertise, BDITEXP: Female board directors with IT expertise, BINDITEXP: Independent board directors with IT expertise, BCCG: Board commitment to cybersecurity governance, NIS: NIS regulation, FSIZE: Firm size, INTAN: Asset tangibility, LEV: Leverage, MTBV: Growth opportunities, ROE: Profitability, LOSS: Loss, BSIZE: Board size, GOVS: Governance score, BINDE: Board independence, BGD: Board gender diversity. See Appendix 1 for the definitions of each variable. All continuous variables are winsorized at the 1st and 99th percentiles.

Table 3: Analysis of corporate cybersecurity disclosures: A yearly industry breakdown

Industry	Year							Total
	2015	2016	2017	2018	2019	2020	2021	
Basic Materials	2.231	4.231	7.214	7.214	7.286	9.571	15.533	7.784
Consumer Discretionary	4.429	6.933	8.478	10.292	11.30	12.922	15.137	10.144
Consumer Staples	3.95	5.278	6.895	7.25	8.00	13.20	14.00	8.423
Energy	5.714	5.429	8.625	7.75	8.875	10.25	16.778	9.327
Financials	3.806	5.161	5.991	5.861	6.617	9.328	10.155	6.815
Health Care	4.545	5.00	9.364	11.727	11.818	14.091	15.273	10.26
Industrials	6.321	7.929	9.143	9.089	11.807	14.912	18.614	11.147
Real Estate	2.174	3.75	4.222	6.074	8.071	9.00	12.286	6.703
Technology	2.857	5.714	13.714	10.429	14.429	27.70	35.50	17.491
Telecommunications	13.25	12.50	16.20	17.20	17.167	29.50	34.167	20.972
Utilities	6.429	8.143	12.143	14.00	12.143	14.571	18.571	12.286
Total	4.419	5.967	7.532	7.972	9.177	12.246	14.603	8.998

* Note: CSD in this table is measured by number of sentences

Table 4: Pairwise correlations matrix

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
(1) CSD	1.000												
(2) BCCG	0.373***	1.000											
(3) NIS	0.2***	0.334***	1.000										
(4) FSIZE	0.115***	0.142***	0.078***	1.000									
(5) INTAN	0.186***	0.198***	-0.017	0.010	1.000								
(6) LEV	0.027	0.101***	0.058***	0.371***	0.085***	1.000							
(7) MTBV	0.04*	0.032	-0.001	-0.092***	0.026	0.089***	1.000						
(8) ROE	0.114***	0.043**	-0.09***	-0.136***	0.019	-0.029	0.115***	1.000					
(9) LOSS	0.025	-0.044**	-0.104***	-0.037*	0.003	-0.117***	0.015	0.543***	1.000				
(10) BSIZE	0.22***	0.212***	0.028	0.66***	0.241***	0.285***	-0.021	-0.019	-0.027	1.000			
(11) GOVS	0.183***	0.233***	0.125***	0.382***	0.224***	0.192***	0.006	0.024	0.048**	0.475***	1.000		
(12) BINDE	-0.047**	-0.023	0.174***	0.003	-0.224***	-0.165***	-0.033	-0.093***	-0.046**	-0.334***	-0.196***	1.000	
(13) BGD	0.184***	0.268***	0.413***	0.086***	-0.026	0.033	0.004	0.087***	0.007	-0.011	0.193***	0.286***	1.000

Notes: This table presents the Pearson correlation matrix for all variables used in our main empirical models. CSD: Corporate cybersecurity disclosures, BCCG: Board commitment to cybersecurity governance, NIS: NIS regulation, FSIZE: Firm size, INTAN: Asset tangibility, LEV: Leverage, MTBV: Growth opportunities, ROE: Profitability, LOSS: Loss, BSIZE: Board size, GOVS: Governance score, BINDE: Board independence, BGD: Board gender diversity. See Appendix 1 for the definitions of each variable. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Table 5: The impact of board commitment to cybersecurity on corporate cybersecurity disclosures

Model (Variables)	(1) CSD	(2) CSTI	(3) CRMT
BCCG	3.010*** (0.002)	0.442*** (0.001)	0.736*** (0.002)
FSIZE	-0.578* (0.003)	-0.088 (0.001)	-0.193 (0.002)
INTAN	0.679*** (0.001)	0.288*** (0.008)	0.226* (0.002)
LEV	-0.045 (0.003)	-0.009 (0.001)	-0.002 (0.003)
MTBV	0.152 (0.009)	0.026 (0.004)	0.134** (0.005)
ROE	0.687*** (0.008)	0.068 (0.007)	0.221** (0.001)
LOSS	-0.007 (0.001)	-0.006 (0.005)	-0.003 (0.007)
BSIZE	0.010*** (0.002)	0.002*** (0.001)	0.005*** (0.001)
GOVS	0.237 (0.017)	0.238*** (0.008)	0.107 (0.011)
BINDE	0.073 (0.024)	-0.230** (0.010)	-0.248 (0.015)
BGD	0.280*** (0.032)	0.027 (0.015)	0.474** (0.022)
Year fixed effect	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes
Constant	0.107*** (0.037)	0.267 (0.018)	0.197 (0.027)
Observations	1,877	1,877	1,877
Adj. R-squared	0.175	0.103	0.125

Notes: This table presents the impact of board commitment to cybersecurity on corporate cybersecurity disclosures. The analysis of overall CSD and its subcategories, CSTI and CRMT, is provided in Columns 2 and 3, respectively. CSD: Corporate cybersecurity disclosures, CSTI: Cybersecurity threats and incidents, CRMT: Cybersecurity risk mitigation and technologies, BCCG: Board commitment to cybersecurity governance, FSIZE: Firm size, INTAN: Asset tangibility, LEV: Leverage, MTBV: Growth opportunities, ROE: Profitability, LOSS: Loss, BSIZE: Board size, GOVS: Governance score, BINDE: Board independence, BGD: Board gender diversity. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors are reported in parentheses. All continuous variables are winsorized at the 1st and 99th percentiles. See Appendix 1 for the definitions of each variable.

Table 6: The impact of board commitment to cybersecurity and NIS regulation on corporate cybersecurity disclosures

Model (Variables)	(1) CSD	(2) CSTI	(3) CRMT
BCCG	2.782*** (0.004)	0.312** (0.002)	0.327*** (0.003)
NIS	0.260*** (0.008)	0.110*** (0.006)	0.392*** (0.009)
BCCG * NIS	0.278** (0.050)	0.194 (0.021)	0.613*** (0.031)
FSIZE	-0.508* (0.003)	-0.080 (0.001)	-0.169 (0.002)
INTAN	0.732*** (0.002)	0.289*** (0.084)	0.230* (0.001)
LEV	-0.052 (0.036)	-0.092 (0.016)	-0.021 (0.023)
MTBV	0.157* (0.094)	0.027 (0.039)	0.137** (0.058)
ROE	0.766*** (0.001)	0.068 (0.077)	0.221** (0.001)
LOSS	-0.647 (0.012)	-0.639 (0.005)	-0.267 (0.007)
BSIZE	0.988*** (0.002)	0.249*** (0.001)	0.451*** (0.001)
GOVS	0.180 (0.002)	0.233*** (0.081)	0.089 (0.001)
BINDE	0.0315 (0.001)	-0.227** (0.001)	-0.237 (0.002)
BGD	0.902*** (0.003)	0.0319 (0.002)	0.485** (0.001)
Year fixed effect	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes
Constant	0.975*** (0.038)	0.490 (0.019)	1.285** (0.027)
Observations	1,877	1,877	1,877
Adj. R-squared	0.180	0.103	0.127

Notes: The impact of board commitment to cybersecurity and NIS regulation on corporate cybersecurity disclosures. The analysis of overall CSD and its subcategories, CSTI and CRMT, is provided in Columns 2 and 3, respectively. CSD: Corporate cybersecurity disclosures, CSTI: Cybersecurity threats and incidents, CRMT: Cybersecurity risk mitigation and technologies, BCCG: Board commitment to cybersecurity governance, NIS: NIS regulation, BCCG * NIS: the interaction of Board commitment to cybersecurity governance and NIS regulation, FSIZE: Firm size, INTAN: Asset tangibility, LEV: Leverage, MTBV: Growth opportunities, ROE: Profitability, LOSS: Loss, BSIZE: Board size, GOVS: Governance score, BINDE: Board independence, BGD: Board gender diversity. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors are reported in parentheses. All continuous variables are winsorized at the 1st and 99th percentiles. See Appendix 1 for the definitions of each variable.

Table 7: Robustness Check: Testing Subsamples Based on corporate governance, firm size and profitability

Model (Variables)	(1) CSD Strong governance	(2) CSD Weak governance	(3) CSD Big size firms	(4) CSD Small size firms	(5) CSD High-performing firms	(6) CSD Low-performing firms
BCCG	2.807*** (0.327)	3.694*** (0.345)	2.588*** (0.040)	3.010*** (0.029)	2.936*** (0.036)	2.653*** (0.031)
FSIZE	0.398 (0.004)	-0.262*** (0.005)	-0.347 (0.004)	-0.481*** (0.007)	-0.176*** (0.005)	0.563 (0.003)
INTAN	0.124*** (0.002)	-0.375 (0.001)	0.125*** (0.001)	0.013 (0.002)	0.110*** (0.003)	0.0647*** (0.002)
LEV	-0.007 (0.004)	0.006 (0.005)	-0.003 (0.004)	-0.001 (0.006)	-0.008 (0.001)	-0.045 (0.002)
MTBV	0.003* (0.001)	0.002 (0.002)	0.007 (0.007)	-0.003 (0.004)	0.005 (0.001)	0.023* (0.001)
ROE	0.612** (0.002)	0.761*** (0.003)	-0.053 (0.006)	0.655*** (0.008)	0.677** (0.002)	-0.357 (0.005)
LOSS	-0.019 (0.017)	0.094 (0.016)	0.010 (0.018)	0.019 (0.016)	0.017 (0.028)	0.012 (0.014)
BSIZE	0.010*** (0.003)	0.014*** (0.003)	0.079*** (0.029)	0.085*** (0.009)	0.079** (0.008)	0.087*** (0.002)
GOVS	0.507 (0.005)	0.688* (0.003)	0.738** (0.008)	0.567 (0.007)	0.165 (0.003)	0.269 (0.002)
BINDE	-0.104 (0.004)	-0.003 (0.003)	0.247 (0.004)	-0.141 (0.003)	0.387 (0.004)	0.237 (0.006)
BGD	0.083 (0.005)	0.172*** (0.003)	0.372 (0.006)	0.880*** (0.002)	0.128** (0.001)	0.132*** (0.004)
Year fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Constant	0.0143 (0.055)	0.366*** (0.063)	0.0589 (0.068)	0.706*** (0.099)	0.274*** (0.066)	0.0722 (0.048)
Observations	1,080	797	847	1,030	820	1,057
Adj. R-squared	0.149	0.239	0.130	0.256	0.174	0.203

*Notes: This table presents the results of a robustness test of our main findings by analyzing three subsamples based on corporate governance strength, firm size, and profitability. Columns 1 and 2 present the results for firms with strong and weak governance, respectively. Columns 3 and 4 focus on large and small-sized firms, while Columns 5 and 6 provide the analysis for high-performing and low-performing firms. CSD: Corporate cybersecurity disclosures, CSTI: Cybersecurity threats and incidents, CRMT: Cybersecurity risk mitigation and technologies, BCCG: Board commitment to cybersecurity governance, FSIZE: Firm size, INTAN: Asset tangibility, LEV: Leverage, MTBV: Growth opportunities, ROE: Profitability, LOSS: Loss, BSIZE: Board size, GOVS: Governance score, BINDE: Board independence, BGD: Board gender diversity. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors are reported in parentheses. All continuous variables are winsorized at the 1st and 99th percentiles. See Appendix 1 for the definitions of each variable.*

Table 8: Robustness Check: Alternative Measures of CSD, BCCG, and Lagged CSD–BCCG Relationships

Model (Variables)	(1) LogCSD	(2) LogCSTI	(3) LogCRMT
<i>Panel A: Alternative measures of Corporate Cybersecurity Disclosures</i>			
BCCG	3.381*** (0.035)	1.486*** (0.033)	2.532*** (0.034)
NIS	0.561*** (0.011)	0.202* (0.012)	0.502*** (0.011)
BCCG*NIS	2.722** (0.044)	0.909 (0.042)	2.196*** (0.042)
Controls	Included	Included	Included
Year fixed effect	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes
Constant	2.754*** (0.538)	0.205 (0.542)	2.438** (0.541)
Wald test	3.76	2.21	3.33
Pseudo R-squared	0.117	0.098	0.085
Observations	1,877	1,877	1,877
<i>Panel B: Alternative measures of BCCG</i>			
Model (Variables)	(1) CSD	(2) CSTI	(3) CRMT
BCCG	2.97*** (0.002)	0.596*** (0.001)	0.114*** (0.001)
NIS	1.420*** (0.001)	0.590** (0.007)	0.730** (0.001)
BCCG*NIS	2.390** (0.002)	0.501 (0.001)	0.957*** (0.002)
Controls	Included	Included	Included
Year fixed effect	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes
Constant	0.667* (0.037)	0.260 (0.016)	0.413* (0.023)
Adj. R-squared	0.188	0.126	0.130
Observations	1,877	1,877	1,877
<i>Panel C: Lagged CSD– BCCG structure</i>			
Model (Variables)	(1) CSD	(2) CSTI	(3) CRMT
BCCG	0.593** (0.028)	0.248** (0.012)	0.0449*** (0.015)
NIS	0.561*** (0.011)	0.202* (0.011)	0.502*** (0.013)
BCCG*NIS	1.770* (0.041)	0.113 (0.424)	1.840** (0.0419)
Controls	Included	Included	Included
Year fixed effect	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes
Constant	1.186** (0.549)	0.157** (0.546)	1.628** (0.545)
Adj. R-squared	0.158	0.104	0.113

Observations	1,617	1,617	1,617
--------------	-------	-------	-------

*Notes: This table presents the results of robustness checks using alternative measures of corporate cybersecurity disclosures (CSD), board commitment to cybersecurity governance (BCCG), and the lagged CSD–BCCG relationship. Panel A focuses on alternative measures of CSD, with Columns 1, 2, and 3 reporting results for LogCSD, LogCSTI, and LogCRMT, respectively. Panel B explores alternative measures of BCCG, with Columns 1, 2, and 3 reporting results for CSD, CSTI, and CRMT, respectively. Panel C examines the lagged CSD–BCCG structure, with Columns 1, 2, and 3 again presenting results for CSD, CSTI, and CRMT. CSD: Corporate cybersecurity disclosures, CSTI: Cybersecurity threats and incidents, CRMT: Cybersecurity risk mitigation and technologies, BCCG: Board commitment to cybersecurity governance. All models include the NIS regulation (NIS), an interaction term between BCCG and NIS, and control variables. Year and industry fixed effects are also incorporated across all panels. Robust standard errors are reported in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors are reported in parentheses. All continuous variables are winsorized at the 1st and 99th percentiles. See Appendix 1 for the definitions of each variable.*

Table 9: Robustness Checks: 2SLS, 3SLS, and Heckman Two-Stage Models

Model (Variables)	(1) 2SLS	(2) 3SLS	(3) Heckman 1st stage	(4) Heckman 2nd stage
BCCG	0.162*** (0.019)	6.185*** (0.717)		2.254*** (0.262)
MILLS				0.070*** (0.011)
Controls	Included	Included	Included	Included
Year fixed effect	Yes	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes	Yes
Constant	-0.023*** (0.006)	-0.033*** (0.004)	-1.555*** (0.595)	0.222*** (0.041)
Adj. R-squared	0.124	0.103		0.193
Observations	1,877	1,877	1,877	1,877
F-test	170.364	124.510		
Prob>F	0.000***	0.000***		
Test of endogeneity (p-value)	0.000			
F-test (First stage)	0.000	0.000		
Breusch-Pagan LM (p-value)		0.000		

*Notes: This table reports regression results from 2SLS, 3SLS, and Heckman two-stage models examining the relationships between board commitment to cybersecurity governance (BCCG) and cybersecurity disclosure (CSD). All models include control variables, year fixed effects, and industry fixed effects. Additional diagnostic tests, including the F-test, the test of endogeneity, and the Breusch-Pagan LM test. Robust standard errors are reported in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors are reported in parentheses. All continuous variables are winsorized at the 1st and 99th percentiles. See Appendix 1 for the definitions of each variable.*

Table 10: Difference-in-differences analysis

Panel A: Pre-match Diagnostic Test				
Variable	Treated	Control	t-test	P-value>t
FSIZE	15.393	14.982	-3.429	0.001
INTAN	27.985	15.709	-8.209	0.000
LEV	117.214	68.290	-6.448	0.000
MTBV	-0.778	4.230	1.919	0.055
ROE	15.584	15.388	-0.120	0.905
LOSS	0.807	0.869	2.548	0.011
BSIZE	9.457	8.488	-5.685	0.000
GOVS	64.512	57.866	-4.071	0.000
BINDE	62.400	69.392	5.965	0.000
BGD	30.381	29.358	-1.247	0.213
Panel B: Post-match Diagnostic Test				
Variable	Treated	Control	t-test	P-value>t
FSIZE	15.384	15.340	0.250	0.806
INTAN	27.915	28.202	-0.130	0.896
LEV	118.610	118.050	0.040	0.967
MTBV	4.522	4.217	0.410	0.682
ROE	15.139	12.854	0.850	0.398
LOSS	0.807	0.807	0.000	1.000
BSIZE	9.446	9.614	-0.780	0.437
GOVS	64.461	65.616	-0.620	0.536
BINDE	62.423	61.157	1.020	0.308
BGD	30.333	28.864	1.390	0.166
Panel C: DiD Effect on CSD				
Variables	CSD			
Post	0.357** (0.014)			
Treatment firms	0.648*** (0.007)			
Post*Treatment firms	0.346** (0.020)			
Controls	Included			
Year fixed effect	Yes			
Industry fixed effect	Yes			
Constant	0.133*** (0.004)			
Adj. R-squared	0.196			
Observations	1,063			

Notes: This table presents the results of a difference-in-differences (DiD) analysis. Panel A provides the pre-match diagnostic test. Panel B presents the post-match diagnostic test. Panel C reports the DiD estimation results. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors are reported in parentheses. All continuous variables are winsorized at the 1st and 99th percentiles. See Appendix 1 for the definitions of each variable.

Appendices

Appendix 1: Variable definitions

Variables	Symbols	Definitions
Corporate Cybersecurity Disclosures (%)	CSD	The percentage of the number of CSD sentences scaled by the total number of sentences in the annual report.
Cybersecurity Threats and Incidents (%)	CSTI	The percentage of the number of cybersecurity threats and incidents-related sentences reported in the annual report based on our primary keyword list, where each sentence refers to the cybersecurity threats and risks.
Cybersecurity risk mitigation and technologies (%)	CRMT	The percentage of the number of cybersecurity risk mitigation and technologies-related sentences reported in the annual report based on our primary keyword list, where each sentence refers to the technologies, processes, and practices implemented to safeguard networks, devices, software, and information from unauthorized access, harm, or attacks.
Cybersecurity Policy	FCSP	A dummy variable equals 1 if the firm have a policy on cyber security in place to protect from cyber-attack, unauthorized access & data leaks, etc., and 0 otherwise.
Board IT Committee	BITC	A dummy variable equals 1 if the firm has a board committee responsible for cybersecurity, and 0 otherwise.
Board IT expertise	BITEXP	The proportion of board members who possess expertise in information technology (IT).
Female board directors with IT Expertise	BDITEXP	The percentage of female board members who possess expertise in IT.
Independent board directors with IT Expertise	BINDITEXP	The percentage of independent board members who have expertise in IT expertise.
Board commitment to cybersecurity governance	BCCG	The board's commitment to cybersecurity governance is measured by a composite score, developed using Principal Component Analysis (PCA) from five variables: FCSP, BITC, BITEXP, BDITEXP, and BINDITEXP. A higher score indicates greater cybersecurity commitment by the board.
NIS regulation	NIS	A dummy variable, equals to 1 for post-2018 (2019 to 2021); 0 for pre-2018 (2015–2018).
Firm size	FSIZE	Natural logarithm of total assets of the firm.
Asset tangibility	INTAN	Natural logarithm of intangible assets.
Leverage	LEV	Percentage of total debt to total assets.
Growth opportunities	MTBV	Percentage of market to book value of equity.
Profitability	ROE	Percentage of net income to total equity.
Loss	LOSS	A dummy variable equals 1 if the firm reports negative net income in year t, 0 otherwise.
Board size	BSIZE	Number of board directors
Governance score	GOVS	Firm-specific governance performance score based on the Asset4 database of Refinitiv Eikon.
Board independence	BINDE	Percentage of independent directors on board of a firm.
Board gender diversity	BGD	Percentage of female directors on the board

Note: This table provides full definitions of all variables included in the empirical models.

Appendix 2: List of keywords used for cybersecurity disclosures analysis

This appendix provides the primary keywords used to identify and categorize cybersecurity disclosures in the annual reports of UK FTSE 350 firms. The keywords are divided into two main categories: Cybersecurity Threats and Incidents (CSTI) and Cybersecurity Risk Mitigation and Technologies (CRMT). These keywords were used in the textual analysis to capture the extent and nature of cybersecurity information disclosed by firms.

CSD Categories	Primary Keyword List
CSTI	'cyber attack,' 'cyber fraud,' 'cyber threat,' 'cyber risk,' 'cyber terrorist,' 'cyber incident,' 'cyber exposure,' 'cyber criminals,' 'security breach,' 'breach in security,' 'security incident,' 'data breach,' 'unauthorised access,' 'unauthorised disclosure,' 'data corruption,' 'corruption of data,' 'network break-in,' 'computer virus,' 'computer breach,' 'computer break-in,' 'computer attack,' 'intrusion,' 'hacking,' 'hacker,' 'denial of service,' 'information technology attack,' 'data theft,' 'phishing,' 'malware,' 'espionage,' 'crimeware,' 'ransomware,' 'keylogger,' 'keystroke logging,' 'social engineering,' 'information loss.'
CRMT	'cyberspace,' 'encryption,' 'network security,' 'security management,' 'information security,' 'cyber insurance,' 'computer security,' 'data confidentiality,' 'confidentiality of data,' 'confidential data,' 'TPSPs maintenance,' 'authentication system,' 'data safe haven,' 'cyber liaison officer,' 'CLO,' 'websense,' 'infosec,' 'system security,' 'information technology security.'

Note: We also used different variants of the word combinations, such as 'cyber attack,' 'cyber-attack,' and 'cyberattack.'

Appendix 3: Examples of excerpts from annual reports referring to cybersecurity disclosures

Company	Year	Industry	Examples of Cybersecurity Disclosures (CSD)	CSD Category
Aviva Plc	2015	Insurance	"During the year, market conditions generally have offered some challenges and the acquisition and integration of the Friends Life business, ensuring our readiness for Solvency II (SII) and the evolving cyber risk environment have all required close attention. (Page 88)" "The Committee monitored certain Major Control Improvement Topics identified by management namely, IT security, disaster recovery in UK datacentres, GI underwriting risk accumulation and outsourcing. Actions on these topics include the provision of more detailed controls on information security, business continuity and physical security, the completion of a GI risk accumulation data accuracy and capture project, and work to improve the management and oversight of outsourcing arrangements Group-wide. (Page 90)"	CSTI CRMT
Big Yellow Group Plc	2016	Real Estate	"The Group receives specialist advice and consultancy in respect of cyber security and we have dedicated in-house monitoring and regular review of our security systems, we also limit the retention of customer data to the minimum requirement. (Page 21)" "During the year we have continued to invest in digital security. Some of the changes include more frequent penetration testing of internet facing systems, adding components such as anti-ransomware as well as the maintenance replacement of components (such as firewalls) to the latest technology and specification. (Page 21)"	CSTI CRMT
Currys Plc	2017	Retail	"The work programme will continue to be responsive to the changing risk landscape, the developing business model, the regulatory environment, and the changing shape of the systems (including IT) architecture. In particular, the Committee will continue to receive reports and updates from management on the IT security improvement actions and plans. In light of the recent data breach, these have been re-assessed and accelerated. (Page 51)" "The security of our data is also hugely significant to the business and in light of the unauthorised data access we recently became aware of, we will further bolster our information security capabilities and review procedures by improving IT security controls, training, monitoring, testing and oversight. (Page 4)"	CSTI CRMT
BT Group Plc	2018	Telecommunications	"We have compartmentalised our IT estate as we provision new cloud-based systems to limit the potential impact of a cyber attack. (Page 51)"	CSTI

			"Cyber and information security: Security risks could arise from people inside BT or from external sources like hacktivists, criminals, terrorists or nation states attacking our infrastructure and assets, for example through use of hacking tools, phishing scams and disruptive malware. (Page 51)"	CRMT
Derwent London Plc	2019	Real Estate	"The Committee reviews a dashboard of key risk indicators at each meeting which includes information security and cyber risk-related KPIs. During 2019, there were 201,532 (2018: 474) attempted attacks on our systems, none of which resulted in a security breach and 99.98% (2018: 99.9%) of the attempts were stopped before they reached the intended targets – this highlights the robustness of our cyber security posture." "All staff attend mandatory information security workshops each year which focus on our policies and procedures, cyber and personal security. Our Group intranet also includes a ‘tips and tricks’ section for our staff with guidance on issues such as cyber security, social media and general security awareness."	CSTI
Experian Plc	2020	Business Services	"We gather intelligence to help our security teams stay ahead of evolving cyber threats. This year, we expanded our interaction with law enforcement authorities and others in our industry to help give each other early warnings of high-potential cyber security threats. (Page 43)" "We have a comprehensive Global Security Policy and controls based on the internationally recognised ISO 27001 standard. Our robust information security programme builds on industry-recognised procedures, including the US National Institute of Standards and Technology (NIST) framework. (Page 44)"	CRMT
Marshall Plc	2021	Industrials	"The Committee is pleased to report that, although the wider risk of cyber fraud continues to increase, no significant failings or weaknesses were identified during the year and the Group’s significant investments in enhanced cyber security measures and systems have enhanced its maturity in this area. There were no incidences of fraud that significantly affected the Group’s business during 2021. (Page 90)" "Appropriate tools and training procedures are in place to protect sensitive data when stored and transmitted between parties (e.g. encryption of hard drives, restricted USB devices, secure data transmission mechanisms and third-party security audits). (Page 38)"	CSTI
				CRMT