Cybersecurity Incidents, Stock Price Synchronicity, and the Role of ESG: Evidence from Taiwan

1. Introduction

In the digital age, cybersecurity incidents have emerged as a critical concern for organizations across the globe. According to the Data Breach QuickView report released at the end of 2021, approximately 4,145 companies worldwide publicly disclosed data breaches, affecting around 22 billion data records.[1] These incidents, primarily caused by cyberattacks, viruses, web exposures, and email leaks, pose significant threats not only to organizational integrity but also to financial performance and investor confidence. In Taiwan, at least 14 companies report substantial cybersecurity incidents in 2021 alone, highlighting the urgency of addressing these vulnerabilities in a rapidly evolving digital landscape.[2] Cybersecurity incidents severely impact companies, causing damage to reputation and goodwill, loss of customers, reduced productivity, and higher operational costs. These factors collectively affect cash flow and overall performance, ultimately resulting in declines in stock prices.[3]

The financial consequences of cybersecurity incidents can extend beyond immediate stock price reductions. These events may significantly alter **s**tock price

[1] https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/; http://blog.nsfocus.net/rbs-data-security/

[2] For example, on March 20, 2021, the ransomware group REvil claimed responsibility for hacking Acer, demanding a ransom of $50 million USD (around 14 billion NTD) and publishing screenshots of allegedly stolen data. This incident demonstrates the high stakes of ransomware attacks but also reveals Acer's robust cybersecurity management. Acer reportedly handles the situation effectively and refuses to pay the ransom, showcasing resilience and a potentially well-structured cybersecurity system. Another incident occurred on October 19, 2021, further underlining the importance of continuous cybersecurity vigilance. Both incidents draw attention internationally, with details disclosed on cybersecurity platforms, highlighting how cybersecurity incidents can serve as tests of a company's governance and crisis management. These events emphasize that cybersecurity incidents do not solely signify losses; they can also reflect the adequacy of a company's information security practices. For further details, refer to these sources: https://www.ithome.com.tw/news/149271; https://www.ithome.com.tw/news/143355.

[3] Janakiraman et al. (2018) found that data breach announcements lead to a decrease in customer spending, underscoring the negative impact of such breaches on customer trust and purchasing behaviors. Makridis and Dean (2018) discussed how data breaches can lead to decreased productivity and increased operational costs. Tosun (2021) found that cyberattacks lead to significant increases in operational costs and declines in profitability. Goel and Shawky (2009) demonstrated that security breach announcements are associated with negative abnormal returns, reflecting investor concerns over reputational damages. Cavusoglu et al. (2004), Acquisti et al. (2006), and Kannan et al. (2007) highlighted the negative implications for stock prices post-breach. Goel and Shawky (2009) also found that firms heavily reliant on online operations experience more significant declines in market value, emphasizing the vulnerability of digitally integrated businesses to cybersecurity incidents. Spanos and Angelis (2016) highlighted the role of firm-level characteristics in determining the severity of these impacts. Martin et al. (2017) further showed that data security breaches affect firm performance and create spillover vulnerabilities from rival firm's breaches. Akey et al. (2021) demonstrated that the effects of breaches extend beyond immediate market responses, influencing investor perceptions of long-term risks.

synchronicity through longer-term underperformance and increased volatility (Corbet and Gurdgiev, 2019; Akey et al, 2021; Hogan et al., 2023). According to Roll (1988), stock price fluctuations are influenced by market factors, industry trends, and firm-specific information. Previous studies measure stock price synchronicity using R-squared values from the market model, with lower values indicating firm-specific influences and higher values reflecting market or industry factors. Morck et al. (2000) found that emerging markets exhibit higher stock price synchronicity compared to developed markets. Taiwan's stock market ranks among the top three in terms of price synchronicity, suggesting that the fluctuations of individual stock prices in Taiwan are more susceptible to market or industry factors. When companies make strategic decisions or experience significant events, firm-specific information often influences stock price synchronicity. Prior research highlights various events that affect stock price synchronicity. Events like stock buybacks, credit rating downgrades, and comment letters reduce stock price synchronicity by incorporating firm-specific information, whereas changes that improve market liquidity tend to increase synchronicity.[4]

The relationship between cybersecurity incidents and stock price synchronicity, however, is more complex. When firms disclose such incidents, it may signal internal control problems or operational vulnerabilities, leading investors to rely more on market-wide information rather than firm-specific data. This dynamic can result in increased stock price synchronicity following a cybersecurity incident. However, Kvochko and Pant (2015) and Richardson et al. (2019) found that while the announcement of cybersecurity incidents has a negative impact on stock prices, the effect was relatively small and diminished over time. This suggests that market participants may initially react negatively to such announcements, but as more information becomes available, the influence of firm-specific factors may reassert itself, leading to changes in stock price synchronicity. On the other hand, studies also show that timely and detailed disclosure of firm-specific information can reduce stock price synchronicity by enabling investors to better assess the situation and the company's response (Haggard et al., 2008, Gordon et al., 2010).

Furthermore, cybersecurity issues are closely tied to environmental, social, and governance (ESG) considerations, particularly in corporate governance and risk management. In recent years, Taiwan's Financial Supervisory Commission (FSC) has

[4] Busch and Obernberger (2017) found that share repurchases increase the synchronicity of the repurchasing firm's stock with the market. Xu et al. (2022) found that comment letters embed firm-specific information into stock prices, thereby reducing synchronicity. Abad et al. (2019) observe that credit rating adjustments, particularly downgrades, increase firm-specific information and lower synchronicity. In contrast, changes that enhance liquidity, such as stock splits (Chang et al., 2015) or high-liquidity environments (Chan et al., 2013), tend to diminish firm-specific information and result in higher synchronicity.

required companies to disclose the losses and responses associated with major cybersecurity incidents. Additionally, the 2022 Corporate Governance Evaluation introduced a scoring item for companies that adopt information security management system standards and obtain third-party certifications, further encouraging firms to enhance their cybersecurity management capabilities. Companies with high ESG ratings are often perceived as better equipped to manage reputation risk and maintain transparency, which can enable them to respond swiftly to cybersecurity incidents and potentially mitigate negative market interpretations. This could reduce stock price synchronicity.[5] Conversely, companies with low ESG ratings may exacerbate information asymmetry due to inadequate disclosure or governance deficiencies, leading to heightened market overreaction and increased synchronicity. However, the protective effect of ESG remains a subject of debate, as prior research offers mixed results on whether ESG consistently mitigates risk during crises. While some studies suggest that high ESG performance can provide downside risk protection, others argue that its impact may be context-dependent or limited, potentially influenced by factors such as persistent negative events or misaligned managerial incentives.[6] Therefore, further investigation is necessary to clarify the role of ESG as a moderating factor in the relationship between cybersecurity incidents and stock price synchronicity.

This study investigates the impact of cybersecurity incidents on stock price synchronicity for Taiwanese listed companies from 2016 to 2023. We follow Gul et al. (2010), Xu et al. (2013), An and Zhang (2013), and Xu et al. (2022) to measure stock price synchronicity by calculating the R-squared from the expanded market model regression. A difference-in-difference approach (Rosati et al., 2019, 2022) is employed to compare synchronicity before and after the incident announcement date. Our findings indicate that cybersecurity incidents increase stock price synchronicity, suggesting that these incidents negatively affect a company's reputation, performance, and value. The

[5] Previous literature emphasizes the role of sustainability-related activities, such as corporate social responsibility (CSR) and ESG investments, in building moral capital and mitigating risks during crises. These activities can foster stakeholder loyalty and reduce the negative impact of adverse events (Godfrey, 2005; Gardberg and Fombrun, 2006; Godfrey et al., 2009). For example, Shiu and Yang (2017) found that long-term CSR investments function as a form of insurance, softening the effects of negative events on stock and bond prices. However, this risk-mitigation effect weakens if negative events persist.

[6] Empirical studies on the ability of ESG performance to mitigate risks during crises yield mixed results. During the 2008–2009 financial crisis, ESG performance generally provides downside risk protection (Bouslah et al., 2018; Cornett et al., 2016; Lins et al., 2017), although Berkman et al. (2021) do not observe this effect. Similarly, during the COVID-19 pandemic, firms with higher ESG ratings or better CSR performance often experience smaller stock price declines or higher returns (Albuquerque et al., 2020; Ding et al., 2021; Cheema-Fox et al., 2021; Arora et al., 2022). However, Demers et al. (2021) found no evidence that ESG performance mitigates the pandemic's negative impact on stock returns unless firms also invest heavily in intangible assets, such as R&D and SG&A expenses. These inconsistencies suggest that the risk-mitigation effects of ESG investments may depend on specific contexts and complementary corporate strategies.

occurrence of a cybersecurity incident signals internal control issues, prompting earnings management or manipulation of disclosure timing to reduce the perceived damage, raising information asymmetry and diminishing the explanatory power of rim-specific information. Consequently, stock price fluctuations are driven more by market factors, leading to increased synchronicity. Furthermore, the effect is more pronounced when companies provide detailed disclosures about the incidents in their annual reports.

We further examine whether the impact of cybersecurity incidents on stock price synchronicity varies based on the company's ESG ratings. The empirical results indicate that, for companies with higher ESG ratings, cybersecurity incidents have a stronger explanatory power over stock price fluctuations. Specifically, for companies with superior ESG performance, stock price synchronicity decreases following a cybersecurity incident. This suggests that firms with better ESG performance can better manage the negative impact of such events, acting as a form of protection against the risk of company collapse (Utz, 2018). Thus, ESG performance functions like insurance. Furthermore, companies with higher ESG ratings often demonstrate greater information transparency, which can serve as an important indicator for investors when evaluating potential investments (Humphrey et al., 2012). As such, ESG performance can enhance the explanatory power of firm-specific information in determining stock price fluctuations (Qiu et al., 2020; Benkraiem et al., 2022). Therefore, for companies experiencing similar cybersecurity incidents, those with better ESG performance are likely to exhibit lower stock price synchronicity.

Next, we investigate whether the impact of cybersecurity incidents on stock price synchronicity differs based on the presence of a Chief Information Security Officer (CISO) and varying levels of financial reporting quality. The empirical results show that, compared to companies without a CISO, firms with a CISO experience a reduction in stock price synchronicity after a cybersecurity incident. Similarly, companies with higher financial reporting quality see a greater decrease in stock price synchronicity following a cybersecurity incident compared to those with lower financial reporting quality. This suggests that companies impacted by cybersecurity incidents may not simply aim to conceal the negative effects. Instead, they may enhance their information security risk assessments post-incident. For instance, they might appoint the CISO to improve information security systems, identify vulnerabilities, and mitigate risks (Shaikh and Siponen, 2023). Additionally, firms may increase the disclosure of qualitative information in financial reports to improve transparency and reduce litigation risks (Bozanic et al., 2017) or strengthen corporate governance mechanisms to lower the likelihood of future internal control deficiencies (Ashraf, 2022). As a result, when more cybersecurity-related details are reflected in stock price fluctuations, stock

price synchronicity tends to decrease following the disclosure of a cybersecurity incident.

Previous studies primarily focus on investors' short-term reactions to cybersecurity incidents using event study methods. This paper extends the analysis to examine the broader impact of such incidents on stock price synchronicity, exploring how ESG performance may moderate this relationship. This research contributes to the literature by highlighting how ESG factors can mitigate the negative impacts of cybersecurity incidents on stock prices. From a policy perspective, the Taiwan Stock Exchange and the Financial Supervisory Commission (FSC) have introduced requirements for companies to disclose material cybersecurity incidents and related impacts in their annual reports. Companies adhering to ISO 27001 and CNS 27001 standards now gain additional corporate governance evaluation points, reflecting a heightened regulatory emphasis on transparency and risk management. This study suggests that cybersecurity incidents convey firm-specific information, aligning with regulatory goals for greater disclosure. Additionally, it emphasizes the synergy between ESG performance and information security, encouraging companies to prioritize ESG initiatives to enhance resilience against adverse events.

The structure of the remaining paper is organized as follows. Section 2 outlines the development of the hypotheses, explaining the theoretical foundations and motivations behind the research questions. Section 3 details the research design, including the sample selection process, variable definitions, and methodological framework. Section 4 presents the empirical results, and Section 5 concludes the paper.

2. Literature Review and Hypothesis Development

2.1 Related Literature on Cybersecurity Incidents

The literature on cybersecurity incidents primarily investigates the market reactions to announcements of such incidents, focusing on short-window reactions. When a company experiences a cybersecurity incident, its value and reputational capital are typically harmed, leading to negative market reactions from investors upon the announcement of the incident (Hung, Huang, and Ku, 2018; Campbell et al., 2003; Cavusoglu et al., 2004; Kannan et al., 2007; Acquisti et al., 2006; Goel and Shawky, 2009; Martin et al., 2017). Kvochko and Pant (2015) and Richardson et al. (2019) found that, although announcements of cybersecurity incidents negatively impact stock prices or cumulative abnormal returns, the effect is relatively small. Gordon et al. (2011) observed that the negative impact on stock prices diminishes over time. Tosun (2021)

found that abnormal returns decrease following announcements of cybersecurity incidents, while trading volume and liquidity increase on the announcement day. Amir, Levi, and Livne (2018) discovered that companies with poor corporate governance, lower litigation risks, and fewer analyst followings are less likely to disclose cyberattack incidents promptly. These companies tend to delay disclosure until the incidents are detected by external parties. On average, they found that investors generally exhibit negative reactions to cybersecurity incidents. However, companies that disclose such incidents promptly face less severe negative reactions compared to those that fail to disclose or delay disclosure. This indicates that withholding information about negative cybersecurity incidents is perceived as more serious by investors, resulting in stronger negative reactions. Foerderer and Schuetz (2022) found that while market investors exhibit negative reactions to cybersecurity incidents, companies can mitigate these reactions by strategically timing the disclosure of such incidents. For example, disclosing incidents during periods when the media is preoccupied reduces media and investor attention, thereby lessening the negative market impact.

When a corporation encounters cybersecurity issues, it frequently has adverse economic repercussions. Lawrence, Minutti-Meza, and Vyas (2018) utilized data breaches to assess the severity of operational control risk. They found that these intrusions impair internal controls over financial reporting (ICFR), indicating that cybersecurity incidents negatively affect ICFR. Stoel and Muhanna (2011) and Heninger, Johnson, and Kuhn (2018) found that firms exhibiting information technology-related material weaknesses (ITMW) generally demonstrate inferior performance. As a result, organizations impacted by cybersecurity breaches may resort to earnings management to obscure their underperformance (Xu, Guo, Haislip, and Pinsker, 2019; He, HuangFu, and Walton, 2022). Xu et al. (2019) discovered that firms encountering cybersecurity issues are predisposed to undertake real profits management to alleviate adverse effects on performance. They additionally noted that occurrences pertaining to financial information exert a more significant impact on earnings management. He et al. (2022) investigated the influence of cybersecurity incidents affecting customers and suppliers on the earnings management practices of other firms in the supply chain. According to transaction cost theory, it was determined that when customers or suppliers encounter cybersecurity events, organizations utilize real earnings management to diminish transaction costs and alleviate the adverse spillover effects resulting from these incidents.

However, the impact of cybersecurity incidents on financial reporting quality is not always negative. Researchers have found that when auditors go to companies that

have had problems in the past, they pay more attention to risk planning and work harder, which leads to higher audit fees (Rosati, Gogolin, and Lynn, 2019; Li, No, and Boritz, 2020). Rosati, Gogolin, and Lynn (2022) found that auditors increase their audit efforts for companies affected by cybersecurity incidents to ensure that the additional costs and the reliability of accounting records are not compromised. Using a difference-in-difference (DID) approach, they found that, after cybersecurity incidents, companies exhibit reduced discretionary accruals, are less likely to report small earnings increases, are more likely to receive going concern opinions, and are less likely to restate financial statements in the two years following the incident. This suggests that auditors improve their risk assessment and implement suitable measures to prevent the incidents from negatively impacting the quality of earnings. These findings suggest that the impact of cybersecurity incidents on earnings quality is not entirely negative.

Companies also respond to cybersecurity incidents by altering their policies. Shaikh and Siponen (2023) found that after experiencing a cybersecurity incident, companies enhance their cybersecurity risk assessments to identify other potential vulnerabilities. This enables them to improve their cybersecurity systems and reduce future risks. Akey, Lewellen, Liskovich, and Schiller (2021) found that companies whose value and reputational capital were hurt by these kinds of incidents actively invest in CSR activities to rebuild intangible assets. They do this to lessen the negative effects of the incidents by being proactive about their CSR involvement. He, Frost, and Pinsker (2020) found that companies tend to reduce R&D expenditures and patent holdings while experiencing decreased investment efficiency but increase cash holdings. These findings indicate that after cybersecurity incidents, companies adopt policies to improve information management systems or adjust investment strategies to lower the risks they might face in the future.

2.2 Related Literature on Stock Price Synchronicity

Roll (1988) proposed that three factors primarily influence stock price volatility: market factors, industry factors, and firm-specific information. Subsequent studies adopted the market model to estimate R^2 as a measure of stock price synchronicity, which serves as an indicator of stock price informativeness. A higher R^2 indicates greater stock price synchronicity, meaning that stock price movements are primarily driven by market and industry information. Conversely, a lower R^2 implies that firm-specific information contributes more significantly to stock price variability, reflecting greater firm-specific information effects. When a firm's disclosed information causes stock price fluctuations, it can impact stock price synchronicity. When R^2 goes down, it means that firm-specific risk is going up and that new information about the firm is getting out, which makes stock prices less likely to move in sync. Morck et al. (2000)

found that in less developed countries with less mature financial environments, R^2 values from the market model are higher, signifying greater stock price synchronicity. This suggests that market and industry factors have relatively higher explanatory power for individual stock price movements in such countries—for example, Taiwan ranks among the top five in terms of stock price synchronicity. Besides differences in how financial markets develop in different countries, other research that looked at what affects stock price synchronicity found that corporate financing decisions, corporate governance, analyst coverage, the quality of financial reporting, and corporate transparency are all important factors.

When a company makes new decisions or experiences specific events, these often imply firm-specific information, which can impact stock price synchronicity. For instance, Busch and Obernberger (2017) found that stock repurchases can speed up and improve the accuracy with which firm-specific information is added to stock prices. This makes stock prices less synchronized. However, de La Bruslerie (2018) did not find evidence that stock repurchases increase the amount of firm-specific information. Chan, Hameed, and Kang (2013) discovered that companies with higher liquidity exhibit less firm-specific information and lower information asymmetry, leading to higher stock price synchronicity. Chang, Lin, and Ma (2015) found that following stock splits, increased stock liquidity and more active market trading decrease the probability of informed trading, thus raising stock price synchronicity. Xu, Huang, and Wen (2022) revealed that companies receiving comment letters experience a decline in stock price synchronicity, indicating that these letters contain firm-specific information that reduces synchronicity.

Abad, Ferreras, and Robles (2019) found that credit rating agency announcements regarding rating changes increase the amount of firm-specific information, thus reducing stock price synchronicity. This effect is more pronounced for rating downgrades, which convey more information compared to upgrades. After notable negative events, such as the bankruptcies of Enron, WorldCom, and Lehman Brothers during the financial crisis, investors began to distrust credit rating agencies. In response, agencies improved their rating mechanisms to restore investor confidence, making credit rating changes after such negative events more informative to investors.

Zheng, Zhang, and Wang (2023) found that heavily polluting firms in China experienced increased stock price synchronicity following the implementation of the Green Credit Policy. This policy likely affects these firms by reducing future operational performance, lowering efficiency, or increasing financing costs, making it more difficult for them to obtain funding (Xu and Li, 2020). To mask the negative impacts of such events, managers may engage in greater earnings management (Lee et

al., 2006) or adopt short-sighted behaviors, which increase the likelihood of managerial expropriation. These actions degrade the quality of information disclosure and diminish the influence of firm-specific information on stock price movements, thereby raising stock price synchronicity.

Generally, when corporate governance is stronger, firm-specific information better explains stock price movements, leading to lower stock price synchronicity. An and Zhang (2013), for example, found that when institutional investors have higher and more stable ownership (longer holding periods), they can make it harder for managers to steal corporate cash flows. This lowers firm-specific risks, raises firm-specific information, and lowers stock price synchronicity. Conversely, when institutional investors have shorter or smaller holdings, their monitoring effectiveness diminishes, and managers are more likely to expropriate corporate cash flows, increasing stock price synchronicity. Boubaker, Mansali, and Rjiba (2014) found that controlling shareholders may obscure firm-specific information. When there is a greater divergence between control rights and cash flow rights, firm-specific information decreases, leading to higher stock price synchronicity. Qiu, Yu, and Zhang (2020), using a sample of Chinese firms, found that companies with higher levels of social trust exhibit lower stock price synchronicity, with the effect being more pronounced in state-owned enterprises (SOEs). Benkraiem, Boubaker, and Saeed (2022) discovered that firms with better CSR performance tend to have greater transparency and provide more firm-specific information, which reduces stock price synchronicity.

Studies on analyst coverage reveal different outcomes across stock markets. For instance, Piotroski and Roulstone (2004), using the U.S. securities market as a sample, found that higher analyst coverage tends to increase industry-level information, thereby raising stock price synchronicity. Conversely, a higher proportion of insiders and institutional investors increases firm-specific information, reducing stock price synchronicity. However, Chan and Hameed (2006), analyzing 26 emerging markets, discovered that greater analyst coverage instead lowers stock price synchronicity. Dang, Dang, Hoang, Nguyen, and Phan (2020) found that media reporting helps firms disclose information, incorporating more firm-specific information into stock price movements. As a result, increased media coverage is associated with lower stock price synchronicity, and corporate governance plays a moderating role, strengthening the negative relationship. Liu and Hou (2019) found that credit trading (measured by accounts payable/total assets, or AP/TA) provides firm-specific information, thereby reducing stock price synchronicity. This effect is more pronounced when customer concentration is higher. However, greater media coverage can mitigate this effect.

If investors lose confidence in firm-specific accounting information or if

information transparency decreases, stock price synchronicity will increase (Bissessur and Hodgson, 2012). Durnev, Morck, and Zarowin (2003) found that voluntary disclosure reduces the cost of acquiring firm-specific information, increases the amount of information related to individual stocks, and lowers stock price synchronicity. In the same way, Jin and Myers (2006) found that higher R^2 is linked to higher information opacity, which can be measured by analyst forecast errors. This means that managers can take advantage of firm cash flows. This reduces the credibility of firm-specific information variability, thereby increasing R^2. Hutton, Marcus, and Tehranian (2009), using discretionary accruals to measure earnings opacity, found that greater opacity reduces the relevance of firm-specific information, leading to higher stock price synchronicity. However, this effect has lessened following the Sarbanes-Oxley Act.

Haggard, Martin, and Pereira (2008) reported similar findings, where greater information opacity increases synchronicity, while greater disclosure decreases it. Cheng, Leung, and Yu (2014) discovered that when firms announce significant earnings surprises, they provide more firm-specific information, resulting in lower stock price synchronicity. This effect is more pronounced for negative earnings surprises. If R^2 effectively captures a firm's information, it should decrease with larger earnings surprises. Bai, Dong, and Hu (2019) found that greater financial statement readability lowers the cost of processing firm-specific information, reducing stock price synchronicity. This effect is stronger in situations with higher information asymmetry, fewer analysts following the firm, or lower institutional ownership. Beuselinck, Jose, Khurana, and Meulen (2009), examining 14 EU countries, found that mandatory adoption of IFRS initially reduced stock price synchronicity in the adoption year but increased it in subsequent years. Bissessur and Hodgson (2012), focusing on Australian firms, reported that stock price synchronicity decreased following mandatory IFRS adoption.

Lower stock price synchronicity indicates that firm-specific information explains a larger portion of stock price movements. Previous studies have shown that higher stock price synchronicity reduces institutional investors' willingness to hold shares (Ting and Huang, 2010) and that stock price synchronicity is negatively related to SEO discounts (Chan and Chan, 2014). Durnev, Morck, and Yeung (2004) found that when stock price synchronicity is lower, more informative stock prices can improve corporate investment efficiency.

In summary, the literature indicates that new information disclosures by firms can influence stock price synchronicity. Morck et al. (2000) noted that Taiwan is a country with relatively high stock price synchronicity, where individual stock prices are more significantly impacted by market and industry information. With the recent rise in

cybersecurity incidents, which not only disrupt business operations but also affect investors, this study looks into whether firms' disclosure of cybersecurity incidents affects stock price synchronicity. The goal is to learn more about how these events affect capital markets.

2.3 Related Literature on ESG

Previous studies suggest that engaging in sustainability-related activities (such as CSR and ESG) can help companies build positive moral capital. During crises, this moral capital enables stakeholders to maintain their loyalty, thereby mitigating the negative impact of adverse events on the company. As a result, ESG engagement can reduce corporate risk (Godfrey, 2005; Gardberg and Fombrun, 2006; Godfrey, Merrill, and Hansen, 2009). Shiu and Yang (2017) found that consistent long-term investment in corporate social responsibility activities can act as a form of insurance during adverse events, reducing the impact on stock prices and corporate bond values. However, if a company repeatedly experiences negative events, this mitigating effect diminishes, supporting the risk mitigation view. From the agency cost perspective, ESG investments may reflect managerial actions driven by personal reputation concerns rather than genuine corporate benefit. In such cases, ESG investments could waste company resources and harm stakeholder wealth. Manchiraju and Rajgopal (2017) found that mandatory increases in CSR expenditures can reduce shareholder value. According to the agency cost view, higher ESG investments could raise corporate risk and lower firm value, which could make stock price or return drops worse during crises. Therefore, whether ESG initiatives can effectively help companies mitigate risks or enhance value during crises requires further investigation.

There is a lot of research that looks at whether ESG can lower company risk during the financial crisis of 2008–2009. Most of it found that ESG performance does lower downside risk during the crisis (Bouslah et al., 2018; Cornett et al., 2016; Lins, Servaes, and Tamayo, 2017). However, Berkman, Li, and Lu (2021) did not find this effect. Alsaifi, Elnahass, and Salama (2020), using a sample of companies listed on the FTSE 350 index on the London Stock Exchange, employed an event study approach to investigate investor reactions to voluntary carbon information disclosures. They found that investors typically responded negatively to carbon disclosures, but during the financial crisis, investors had a positive reaction to carbon disclosures.

The literature exploring whether ESG can mitigate stock price declines during the COVID-19 period has produced inconsistent conclusions. During the first quarter of 2020, the COVID-19 pandemic led to a rapid decline in global stock prices, but ESG funds continued to perform well, sparking widespread discussion about whether ESG

can mitigate the negative impacts of such events. Albuquerque, Koskinen, Yang, and Zhang (2020) found that companies with higher ESG ratings had higher returns during the COVID-19 pandemic. Ding, Levine, Lin, and Xie (2021) also found that companies with better CSR performance had higher returns. Cheema-Fox, LaPerla, Wang, and Serafeim (2021) used a sample of 3,023 global companies and found that, during the COVID-19 pandemic (from February 20, 2020, to March 23, 2020), stock prices generally declined, but companies with higher ESG ratings experienced smaller declines in stock prices. Arora, Sur, and Chauhan (2022) focused on Indian firms and found that during the pandemic, companies with better ESG performance had higher returns than those with poorer ESG performance. Demers, Hendrikse, Joos, and Lev (2021) used both Refinitiv's comprehensive ESG scores and MSCI's ESG ratings to measure ESG performance and explored whether ESG could improve buy-and-hold returns during the pandemic. Unlike previous studies that mainly used E scores, ESG is a more comprehensive measure, but they did not find that ESG could mitigate the decline in buy-and-hold returns during the COVID-19 period. However, they found that companies investing more in intangible assets (measured by R&D and SG&A) could mitigate the negative impact on stock returns during the pandemic.

This study further explores whether the impact of cybersecurity events on stock price synchronicity differs based on the level of ESG ratings.

2.4 Hypothesis Development

When a company experiences a cybersecurity breach, it may face a damaged reputation, additional costs, a negative impact on future revenue, and harm to company value (Akey et al., 2021). Moreover, after a company experiences a cybersecurity breach, market investors typically react negatively. To mitigate the negative impact of cybersecurity incidents, managers may conceal cybersecurity incidents until they can no longer be hidden (Amir et al., 2018) or deliberately manipulate the timing of disclosing cybersecurity incidents to avoid attracting the attention of market investors (Foerderer and Schuetz, 2022), or engage in earnings management to hide poor performance (Xu et al., 2019; He et al., 2022), reducing earnings quality and increasing the likelihood of internal control deficiencies. Cybersecurity incidents can harm internal controls over financial reporting (Lawrence et al., 2018; Xu et al., 2019; He et al., 2022). Therefore, after a company experiences a cybersecurity incident, in order to hide the impact of the negative event, the company may engage in earnings management or manipulate the disclosure timing, which reduces the transparency of company-specific information and earnings quality (Hutton et al., 2009), increases information asymmetry, and thus company-specific information cannot be reflected in

the stock price, increasing stock price synchronicity. That is, after a cybersecurity incident occurs, stock price synchronicity will increase.[7]

However, negative events do not always lead to a decline in financial reporting quality. When companies experience negative events, they may adopt other strategies (other than earnings management) to mitigate the impact of negative events. For example, Bozanic et al. (2017) found that companies that receive comment letters with bad news will increase the disclosure of qualitative information in their financial statements, thereby increasing transparency and reducing the company's litigation risk. Xu et al. (2022) also found that companies that receive negative comment letters will try to correct their financial statements so that company-specific information will increase, reducing stock price synchronicity. After a cybersecurity incident, external auditors may pay more attention to audit risk assessment and put in more effort (Rosati et al., 2019; Li et al., 2020), so companies that have experienced cybersecurity incidents do not have increased earnings management behavior (Rosati et al., 2022). Moreover, Akey et al. (2021) and Makridis and Dean (2018) found that after cybersecurity incidents, companies will increase investment in intangible assets, and Ashraf (2022) explored the spillover effect of cybersecurity incidents and found that when a company experiences a cybersecurity incident, companies in the same industry that do not have cybersecurity incidents are less likely to have internal control deficiencies in the future, indicating that cybersecurity incidents play an important role in improving corporate governance mechanisms. Shaikh and Siponen (2023) found that companies will increase their assessment of information security risks after a cybersecurity incident to identify other weaknesses in the company and improve the company's information security system to reduce risks. Therefore, when companies face the negative impact of cybersecurity incidents, companies that experience cybersecurity incidents may improve information transparency by increasing disclosure to reduce the company's litigation risk or improve information security mechanisms through investment so that cybersecurity incident disclosures can convey information to investors, and cybersecurity incidents are more likely to be reflected in stock price fluctuations, thus reducing stock price synchronicity.

Based on the literature review, the following hypotheses are proposed:

[7] Another perspective is that companies that have experienced cybersecurity incidents usually have weaker internal controls, and therefore the quality of their financial reports is inherently poorer. Even if the company discloses information about the cybersecurity incident and explains the company's response measures, investors may not believe the company's response to the incident due to the weaker internal controls, so the information about the cybersecurity incident may not affect stock price synchronicity.

H1a: *Compared to companies that have not experienced cybersecurity incidents, companies that have experienced cybersecurity incidents will have higher stock price synchronicity after the incident*.

H1b: *Compared to companies that have not experienced cybersecurity incidents, companies that have experienced cybersecurity incidents will have lower stock price synchronicity after the incident*.

Regarding whether ESG can mitigate the negative impact of cybersecurity incidents, based on the insurance-like effects of ESG, if a company experiences a negative event, a better ESG performance can reduce its negative impact and protect shareholder wealth. Qiu et al. (2020) found that companies with higher social trust have lower stock price synchronicity, and this effect is more pronounced for state-owned enterprises (SOEs). Benkraiem et al. (2022) found that companies with better CSR performance have higher transparency and can provide more firm-specific information, thus reducing stock price synchronicity. Moreover, Humphrey et al. (2012) mentioned that CSR information can help investors judge whether a company is a better investment target. Utz (2018) also found that CSR has a risk-mitigation effect in European and American countries, thus reducing crash risk, but in some Asian countries, there is an over-investment effect, which increases crash risk, supporting the over-investment hypothesis. At the same time, it was found that in Europe, Japan, and the United States, when environmental and social performance is better, it can increase firm-specific information, thus reducing stock price synchronicity. Therefore, when a company has better ESG performance, it means that it can improve company transparency and clarify the uncertain relationship between cybersecurity incidents and stock price synchronicity. If cybersecurity incidents cause investors to distrust the company, thus increasing stock price synchronicity, this positive relationship between cybersecurity incidents and stock price synchronicity will be mitigated in companies with better ESG performance; on the other hand, if cybersecurity incidents themselves convey firm-specific information and reduce stock price synchronicity, this negative relationship will be more pronounced in companies with better ESG performance. Hypothesis 2 is as follows:

H2: *The impact of cybersecurity incidents on stock price synchronicity will be more significant when a company has a better ESG rating.*

3. Research Design

3.1 Research Sample and Data Sources

The cybersecurity data used in this study primarily comes from the Taiwan Stock Exchange's Market Observation Post System (MOPS). According to the requirement for listed companies to disclose major information, significant cybersecurity incidents must be publicly disclosed on the MOPS platform. This study collects data on cybersecurity incidents from MOPS, specifically searching for related incidents using keywords such as "hacker", "computer virus infection", "ransomware attack", or "data breach" on the "Major Information and Announcements" webpage.[8] The period for collecting data on cybersecurity incidents in Taiwan's listed companies spans from 2016 to 2023. To compare stock price synchronicity before and after these incidents, data from the years before and after the incidents are included. Therefore, the study sample period ranges from 2013 to 2023. ESG-related data is obtained from the Taiwan Economic Journal (TEJ) "TESG Sustainable Development Indicators" module, while other financial data is sourced from the TEJ financial module, and stock price data comes from the TEJ stock price module.

Table 1 shows the sample selection process. Panel A displays the number of Taiwanese listed companies (excluding the financial industry) for the years 2013-2023, totaling 17,410 company-year observations. After excluding 1,413 observations with missing control variables, the final sample for Hypothesis 1 includes 15,997 company-year observations, of which 532 involve cybersecurity incidents[9], accounting for 3.4% of the total sample (532/15,997). Since ESG-related data begins in 2016, for Hypothesis 2, the sample period starts from 2016. Thus, after excluding 3,903 observations with missing ESG data, the sample for Hypothesis 2 consists of 12,094 observations, with 397 instances of cybersecurity incidents (3.3%). Panel B displays the industry distribution of the Hypothesis 1 sample. Among the companies with cybersecurity incidents, the electronics and electrical machinery industries are the most affected, accounting for 55% (295/532) and 10% (55/532), respectively.

[8] On April 27, 2021, the Taiwan Stock Exchange (TWSE) announced amendments to the procedures for handling material information, explicitly requiring listed companies to disclose significant cybersecurity incidents as material information. This change aimed to address the previous lack of clarity in categorizing cybersecurity breaches under other significant events, which was deemed insufficiently specific. Similarly, on April 29, 2021, the Taipei Exchange (TPEx) updated its public disclosure procedures, requiring the reporting of cybersecurity incidents that caused significant damage or impact as material information. These amendments reflect a growing emphasis on transparency and corporate accountability in response to cybersecurity threats. For further information, refer to the MOPS website.

[9] Since the same company may experience multiple cybersecurity incidents, this study focuses on the first recorded cybersecurity incident for each company to capture its impact on stock price synchronicity more clearly. The empirical dataset comprises a total of 54 firms that have experienced cybersecurity incidents.

[INSERT TABLE 1 ABOUT HERE]

3.2 Research Models and Variable Definitions

3.2.1 Estimating Stock Price Synchronicity

This study follows the approach of Gul et al. (2010), Xu et al. (2013), An and Zhang (2013), and Xu et al. (2022) to estimate stock price synchronicity ($SYNCH$). To avoid the influence of companies that have recently listed or delisted on the estimation of R-squared, this study adopts the method of Morck et al. (2000) and excludes companies with less than 30 weeks of stock trading data. The following Equation (1) is used to calculate the R-squared for each company and each year:

$$RET_{iw} = \alpha_0 + \beta_1 MARKET_w + \beta_2 MARKET_{w-1} + \beta_3 INDRET_w + \beta_4 INDRET_{iw-1} + \varepsilon_{iw} \quad (1)$$

where RET_{iw} is the stock return of company i in week w (weekly returns from Monday to Friday), $MARKET_w$ and $MARKET_{w-1}$ are the market returns in week w and week $w-1$, and $INDRET_w$ and $INDRET_{iw-1}$ are the industry returns in week w and week $w-1$.

To transform the values of R-squared, which range from 0 to 1, into a distribution closer to normal, the natural logarithm is applied. The R-squared estimated from Equation (1) is then transformed using the natural logarithm to obtain $SYNCH$ (Morck et al., 2000):

$$SYNCH_{it} = \ln\left(\frac{R_{it}^2}{1 - R_{it}^2}\right)$$

3.2.2 Research Models

Hypothesis 1 examines the impact of cybersecurity incidents on stock price synchronicity. First, this study employs a difference-in-difference analysis (Rosati et al., 2019; Rosati et al., 2022) to test Hypothesis 1 using the following model:

$$\begin{aligned} SYNCH_{it} = {} & \alpha_0 + \beta_1 BDS_{it} + \beta_2 BDS_{it} \times Post_{it} + \beta_3 SIZE_{it} \\ & + \beta_4 MTB_{it} + \beta_5 Leverage_{it} + \beta_6 ROE_{it} + \beta_7 VOL_{it} + \beta_8 SKEW_{it} \\ & + \beta_9 KURT_{it} + \beta_{10} ZeroReturn_{it} + \beta_{11} TradeVol_{it} + yearFE \\ & + IndustryFE_i + FirmFE_i + \varepsilon_{it} \end{aligned} \quad (2)$$

where $SYNCH_{it}$ is stock price synchronicity, BDS_{it} is a dummy variable where 1 indicates a company experienced a cybersecurity incident, and 0 otherwise. $Post_{it}$ is another dummy variable, set to 1 after the cybersecurity incident occurs and 0 before the incident (Rosati et al., 2019; Rosati et al., 2022). The primary coefficient of interest is β_2. Based on Hypothesis 1a, we expect $\beta_2 > 0$, indicating that after a cybersecurity security incident, stock price synchronicity increases. Conversely, according to Hypothesis 1b, we expect $\beta_2 < 0$, meaning that compared to companies that did not experience an incident, those that did will see a decrease in stock price synchronicity after the event.

Other control variables include: $SIZE_{it}$, which is the natural logarithm of company size (market capitalization), MTB_{it}, the market-to-book ratio, $Leverage_{it}$, the ratio of total liabilities to total assets, ROE_{it}, the return on equity, VOL_{it}, the standard deviation of weekly industry returns, $SKEW_{it}$, the skewness of company weekly returns, and $KURT_{it}$, the kurtosis of company weekly returns. Additionally, following Gassen et al. (2020), this study controls for liquidity by including the ratio of zero-return days to total trading days ($ZeroReturn_{it}$) and the natural logarithm of trading volume ($TradeVol_{it}$). The model also includes year fixed effects ($yearFE$), industry fixed effects ($IndustryFE_i$), and firm fixed effects ($FirmFE_i$).

Hypothesis 2 primarily explores whether the impact of cybersecurity incidents on stock price synchronicity differs based on the level of ESG ratings. To test Hypothesis 2, ESG ratings are divided into two groups based on the median score, with $HighESG_{it}$ set to 1 for companies with higher ESG performance and 0 otherwise. The expectation is that in the group with higher ESG ratings, the impact of cybersecurity incidents on stock price synchronicity will be more pronounced. According to Hypothesis 2, it is expected that better ESG performance will increase the explanatory power of cybersecurity events on stock price synchronicity. The coefficient of $BDS{\times}Post{\times}HighESG$ is expected to be significantly negative, meaning that in the high ESG group, $\beta_4 < 0$. The model for Hypothesis 2 is as follows:

$$\begin{aligned} SYNCH_{it} = {} & \alpha_0 + \beta_1 BDS_{it} + \beta_2 BDS_{it}{\times}Post_{it} + \beta_3 BDS_{it}{\times}HighESG_{it} \\ & + \beta_4 BDS_{it}{\times}Post_{it}{\times}HighESG_{it} + \beta_5 HighESG_{it} + \beta_6 SIZE_{it} \\ & + \beta_7 MTB_{it} + \beta_8 Leverage_{it} + \beta_9 ROE_{it} + \beta_{10} VOL_{it} + \beta_{11} SKEW_{it} \\ & + \beta_{12} KURT_{it} + \beta_{13} ZeroReturn_{it} + \beta_{14} TradeVol_{it} + yearFE \\ & + IndustryFE_i + FirmFE_i + \varepsilon_{it} \end{aligned} \quad (3)$$

4. Empirical Results and Analysis

4.1 Descriptive Statistics and Correlation Coefficients

Panel A of Table 2 presents the descriptive statistics and difference-in-difference tests for all variables in Hypothesis 1. The mean of BDS is 0.033, indicating that approximately 3% of the companies in the sample experienced a cybersecurity incident. The mean and median of stock price synchronicity for all samples are -1.590 and -1.467, respectively. In Panel B, for the subsample of companies with a cybersecurity incident, the mean and median of stock price synchronicity ($SYNCH$) are -1.257 and -1.164, significantly higher than those of the companies without an incident (mean = -1.603, median = -1.483). In terms of differences in control variables, Panel B shows that companies with a cybersecurity incident have significantly higher values for company size ($SIZE$), leverage ratio ($Leverage$), return on equity (ROE), and the natural logarithm of trading volume ($TradeVol$) compared to those without an incident. Meanwhile, companies with an incident have significantly lower values for skewness ($SKEW$), kurtosis ($KURT$), and the ratio of zero return days to total trading days ($ZeroReturn$) compared to companies without an incident. The results from Panel B indicate significant differences in the control variables between companies with and without cybersecurity incidents, so these control variables are included in the model to account for their impact on stock price synchronicity.

[INSERT TABLE 2 ABOUT HERE]

The correlation results (not tabulated) show that except for the correlation between $SKEW$ and $KURT$ (0.563), the absolute values of the correlations between other variables are all below 0.4, indicating that multicollinearity is not a serious issue among the independent variables. To ensure rigor, this study also conducts a Variance Inflation Factor (VIF) test on the subsequent empirical results, with all VIF values being below 5, suggesting that multicollinearity among the variables is not problematic in the regression model.

4.2 Empirical Results and Analysis

Hypothesis 1 examines whether cybersecurity incidents affect the stock price synchronicity of affected companies. The empirical results are presented in Table 3. Column (1) of Table 3 considers only the effect of cybersecurity incidents on stock price synchronicity. The key variables are BDS and $BDS{\times}Post$. The coefficient of BDS is 0.551, with a t-value of 7.152, which is significant at the 1% level. Column (2) adds other control variables and year, industry, and firm fixed effects. The coefficient of BDS is 0.287, with a t-value of 4.011, also significant at the 1% level.

These results suggest that before a cybersecurity incident occurs, companies with such incidents exhibit higher stock price synchronicity compared to those without incidents. Both Column (1) and Column (2) show that $BDS{\times}Post$ is significantly positive, indicating that for companies with a cybersecurity incident, stock price synchronicity increases after the incident. This suggests that after a cybersecurity incident, company-specific information becomes less reflected in stock prices, leading investors to view the company's individual information as less meaningful, thus increasing stock price synchronicity. This result supports Hypothesis 1a.

The other control variables align with previous literature (Gul et al., 2010; An and Zhang 2013; Xu et al., 2013; Xu et al., 2022). Larger companies ($SIZE$) and companies with higher kurtosis ($KURT$) in their weekly returns have higher stock price synchronicity, while companies with higher market-to-book ratio (MTB), leverage ratio ($Leverage$), volatility of industry returns (VOL), skewness in weekly returns ($SKEW$), ratio of zero return days ($ZeroReturn$), and the natural logarithm of trading volume ($TradeVol$) have lower stock price synchronicity.

Hypothesis 2 further investigates whether a company's ESG performance influences the relationship between cybersecurity incidents and stock price synchronicity. In Column (1) of Table 4, ESG is divided into two groups based on the industry median, with a dummy variable ($HighESG$) assigned as 1 if a company's ESG score is above the industry median, and 0 otherwise. The coefficient for $BDS{\times}Post$ is significantly positive, while the interaction term $BDS{\times}Post{\times}HighESG$ is significantly negative (coefficient = -0.306, t-value = -1.826). In Column (2), ESG is treated as a continuous score (ranging from 0 to 100), and the interaction term $BDS{\times}Post{\times}HighESG$ remains significantly negative (coefficient = -0.017, t-value = -1.837). The results from Table 4 suggest that while stock price synchronicity increases following a cybersecurity incident, companies with better ESG performance experience a decrease in stock price synchronicity after such incidents. This implies that cybersecurity incidents lead to a loss of investor trust, which increases stock price synchronicity, but for companies with stronger ESG performance, the positive relationship between security incidents and synchronicity weakens. This supports the notion of ESG providing an "insurance-like effect"—when a company faces negative events, stronger ESG performance can mitigate the negative impacts and protect shareholder wealth.

[INSERT TABLES 3 AND 4 ABOUT HERE]

4.3 Further Analysis

4.3.1 Whether the Company Has a Chief Information Security Officer

To further investigate whether the stock price synchronicity of companies that experience cybersecurity incidents differs depending on whether the company has a CISO, a dummy variable $CISO$ is set to 1 if the company has a CISO, and 0 if not. An interaction term, $BDS{\times}Post{\times}CISO$, is included to test whether having a CISO affects the stock price synchronicity of companies that experience cybersecurity incidents. The empirical results show that the coefficient of the interaction term $BDS{\times}Post{\times}CISO$ is significantly negative (coefficient = -0.937, t-value = -1.740), significant at the 10% level. The results suggest that compared to companies without a CISO, companies with a CISO experience a decrease in stock price synchronicity after a cybersecurity incident. This indicates that companies with cybersecurity incidents do not necessarily aim only to conceal negative impacts. After such incidents, companies may enhance their information security risk assessments and improve their security systems. The establishment of a CISO might help identify other security vulnerabilities and risks (Shaikh and Siponen, 2023). Therefore, after disclosing a cybersecurity incident, the information related to the incident is more likely to be reflected in the stock price fluctuations, leading to a decrease in stock price synchronicity.

[INSERT TABLE 5 ABOUT HERE]

4.3.2 Considering Earnings Quality

Previous literature has found that when a company has poor earnings quality, stock price synchronicity tends to be higher, meaning stock prices reflect less of the company's individual information (Datta et al., 2014). This is consistent with the finding that when auditors are disciplined, the audit process improves, leading to a reduction in discretionary accruals (Carcello et al., 2011; Fung et al., 2017). This study examines whether the decline in stock price synchronicity is more pronounced when a company's earnings quality improves (i.e., discretionary accruals decrease) after an auditor is disciplined. The study uses the level of accrual earnings management (discretionary accruals) to measure the company's financial reporting environment. A lower level of accrual earnings management indicates better earnings quality. Following the method of Kothari et al. (2005), discretionary accruals are estimated using the Modified Jones model, which accounts for performance effects. The coefficients are estimated by industry and year using the following Equation (4), and the estimated coefficients are then used in Equation (5) to calculate discretionary accruals, taking the absolute value ($ABSDA$). Here, TAC refers to total accruals, which are operating income minus operating cash flows. ΔRev represents changes in net

sales, ΔAR represents changes in accounts receivable, PPE is property, plant, and equipment, $Total\ Assets$ is total assets, and ROA is net income after taxes divided by total assets. When the absolute value of discretionary accruals ($ABSDA$) is lower, it indicates better earnings quality.

$$\frac{TAC}{Total\ Assets} = \alpha_0 + \alpha_1 \frac{1}{Total\ Assets} + \alpha_2 \frac{(\Delta Rev - \Delta AR)}{Total\ Assets} + \alpha_3 \frac{PPE}{Total\ Assets} + \alpha_4 ROA + \varepsilon \quad (4)$$

$$ABSDA = \left| \frac{TAC}{Total\ Assets} - \widehat{\alpha_1} \frac{1}{Total\ Assets} + \widehat{\alpha_2} \frac{(\Delta Rev - \Delta AR)}{Total\ Assets} + \widehat{\alpha_3} \frac{PPE}{Total\ Assets} - \widehat{\alpha_4} ROA \right| \quad (5)$$

To further investigate whether the stock price synchronicity of companies that experience cybersecurity incidents differs based on the company's earnings quality, this study creates a financial reporting quality dummy variable (FRQ). If the absolute value of a company's discretionary accruals ($ABSDA$) is below the industry median for the year, FRQ is set to 1, indicating lower earnings management and implying better earnings quality. If the $ABSDA$ is greater than or equal to the industry median for the year, FRQ is set to 0, indicating poorer earnings quality. An interaction term $BDS{\times}Post{\times}FRQ$ is included to test whether the financial reporting environment affects the stock price synchronicity of companies that experience cybersecurity incidents.

The empirical results show that the interaction term $BDS{\times}Post{\times}FRQ$ is significantly negative (coefficient = -0.245, t-value = -1.670), significant at the 10% level. This suggests that, compared to companies with poorer financial reporting quality, companies with better financial reporting quality experience a greater decrease in stock price synchronicity after a cybersecurity incident. The above results indicate that if a company has better earnings quality, the stock price movement after a cybersecurity incident will reflect more company-specific information. This suggests that after a cybersecurity incident, the company may increase the disclosure of qualitative financial information to improve transparency and reduce potential litigation risks (Bozanic et al., 2017) or enhance corporate governance mechanisms to reduce the likelihood of future internal control failures (Ashraf, 2022). After the disclosure of a cybersecurity incident, the information related to the incident is more likely to be reflected in stock price fluctuations, leading to a decrease in stock price synchronicity.

[INSERT TABLE 6 ABOUT HERE]

4.4 Sensitivity Analysis: Propensity-Score Matching (PSM)

Cybersecurity incidents in companies may occur for different reasons. To control for endogeneity factors related to the occurrence of cybersecurity incidents, this study further employs Propensity-Score Matching (PSM) to match companies that have experienced a cybersecurity incident with those that have not. The propensity scores for each sample company in each year are calculated using the following Probit model. Using the method of matching without replacement, a company that did not experience a cybersecurity incident (control group) with the closest propensity score is selected from the same industry in the same year, forming a 1:1 match. After matching, the experimental group (companies that experienced cybersecurity incidents) and the control group form a new sample, and the hypotheses in this study are re-examined using Equations (2) and (3).

$$BDS_{it} = \alpha_0 + \beta_1 TA_{it} + \beta_2 RD_{it} + \beta_3 Leverage_{it} + \beta_4 LOSS_{it} + \beta_5 Risk\_committee_{it} + \beta_6 Tech\_committee_{it} + \varepsilon_{it} \quad (6)$$

In Equation (6), the dependent variable BDS_{it} is a dummy variable indicating whether a cybersecurity incident occurred. If company i experienced a cybersecurity incident in period t, it is set to 1; otherwise, it is set to 0. Control variables include the natural logarithm of total assets at the end of the period (TA), the natural logarithm of research and development expenses (RD), leverage ($Leverage$), reported net loss ($LOSS$), and whether the company has established a risk committee ($Risk\_committee$) or a technology committee ($Tech\_committee$) (He et al., 2022).

The empirical results are presented in Table 7. Column (1) in Panel A presents the results of Hypothesis 1 being re-tested using the propensity-score matched sample. The coefficient of $BDS \times Post$ is significantly positive, indicating that, based on the matched sample, it is still found that the stock price synchronicity of companies that experienced cybersecurity incidents is higher than that of companies that did not experience such incidents, which is consistent with the earlier results, supporting Hypothesis 1a. Hypothesis 2 considers the impact of ESG on the above relationship. From Panel A, Columns (2) and (3), it is found that the coefficient of the interaction term $BDS \times Post \times HighESG$ is significantly negative, suggesting that after a cybersecurity incident, if a company has better ESG performance, it can have an insurance-like effect, encouraging investors to use more company-specific information, thereby reducing stock price synchronicity. Thus, Hypothesis 2 is also supported. Panel B similarly shows that when companies have established a CISO and have better

earnings quality, their stock price synchronicity decreases after a cybersecurity incident, which is consistent with previous conclusions.

[INSERT TABLE 7 ABOUT HERE]

5. Conclusion

This study uses data on cybersecurity incidents from Taiwan-listed companies between 2016 and 2023. Cybersecurity incident data was manually collected from the Taiwan Stock Exchange's public information observation platform, while ESG scores were provided by the TEJ to examine the relationship between ESG, cybersecurity incidents, and stock price synchronicity. To test whether the impact of cybersecurity incidents on stock price synchronicity differs before and after the incidents, this study includes stock returns data from both the years before and after the incidents, with the study period spanning from 2013 to 2023. This study attempts to answer the following questions: (1) Does stock price synchronicity increase or decrease after a company experiences a cybersecurity incident? (2) Does ESG rating affect the relationship between cybersecurity incidents and stock price synchronicity?

The empirical results show that, compared to companies that do not experience cybersecurity incidents, companies that experienced an incident saw an increase in stock price synchronicity. This suggests that after the incident, market investors reduce the use of company-specific information. The likely reason is that cybersecurity incidents negatively affect the company's reputation, performance, and value. Companies involved in such incidents may attempt to manage earnings or adjust the timing of the incident's disclosure to reduce negative perceptions among investors. As a result, earnings quality and information transparency decrease, increasing information asymmetry and reducing the ability of cybersecurity incidents to explain stock price movements, thus raising stock price synchronicity.

The study further explores whether companies that experience cybersecurity incidents but have different ESG ratings exhibit different impacts on stock price synchronicity. It finds that when a company has a better ESG rating, the ability of cybersecurity incidents to explain stock price movements increases. Therefore, in companies with better ESG performance, stock price synchronicity decreases after a cybersecurity incident. This suggests that while such incidents may increase potential risks for the company, a strong ESG performance can act as insurance, improving the explanatory power of the cybersecurity event on stock price movements and reducing stock price synchronicity.

Additionally, for companies that place a higher emphasis on information security investments (e.g., establishing a CISO), their ability to respond to cybersecurity incidents is likely to be better. In these companies, investors may be more willing to believe that they can handle unexpected events or may increase future investments in information security. Therefore, after a cybersecurity incident, such companies may exhibit a greater ability to explain stock price movements, leading to lower stock price synchronicity. Past literature has found that companies involved in cybersecurity incidents often manage earnings to hide the negative impact of the event (He et al., 2022), which reduces earnings quality. This study further finds that if a company initially has good earnings quality, it indicates a lower degree of earnings management. Therefore, companies with better earnings quality experience a decrease in stock price synchronicity after a cybersecurity incident, implying that investors are still willing to use individual company information, thereby lowering stock price synchronicity.

Reference

Abad, P., Ferreras, R., & Robles, M. D. (2019). Informational role of rating revisions after reputational events and regulation reforms. *International Review of Financial Analysis*, 62, 91-103.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94. https://aisel.aisnet.org/icis2006/94.

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2021). Hacking corporate reputations. *Rotman School of Management Working Paper*, 3143740. Available at SSRN: https://ssrn.com/abstract=3143740 or http://dx.doi.org/10.2139/ssrn.3143740.

Albuquerque, R., Koskinen, Y., Yang, S., & Zhang, C. (2020). Resiliency of environmental and social stocks: An analysis of the exogenous COVID-19 market crash. *The Review of Corporate Finance Studies*, 9(3), 593-621.

Alsaifi, K., Elnahass, M., & Salama, A. (2020). Market responses to firms' voluntary carbon disclosure: Empirical evidence from the United Kingdom. *Journal of Cleaner Production*, 262, 121377.

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.

An, H., & Zhang, T. (2013). Stock price synchronicity, crash risk, and institutional investors. *Journal of Corporate Finance*, 21, 1-15.

Arora, S., Sur, J. K., & Chauhan, Y. (2022). Does corporate social responsibility affect shareholder value? Evidence from the COVID-19 crisis. *International Review of Finance*, 22(2), 325-334.

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, 97(2), 1-24.

Bai, X., Dong, Y., & Hu, N. (2019). Financial report readability and stock return synchronicity. *Applied Economics*, 51(4), 346-363.

Benkraiem, R., Boubaker, S., & Saeed, A. (2022). How does corporate social responsibility engagement affect the information content of stock prices?. *Managerial and Decision Economics*, 43(5), 1266-1289.

Berkman, H., Li, M., & Lu, H. (2021). Trust and the value of CSR during the global financial crisis. *Accounting & Finance*, 61(3), 4955-4965.

Beuselinck, C., Joos, P., Khurana, I. K., & Van der Meulen, S. (2009). Mandatory IFRS reporting and stock price informativeness. Available at SSRN 1381242.

Bissessur, S., & Hodgson, A. (2012). Stock market synchronicity–an alternative approach to assessing the information impact of Australian IFRS. *Accounting & Finance*, 52(1), 187-212.

Boubaker, S., Mansali, H., & Rjiba, H. (2014). Large controlling shareholders and stock price synchronicity. *Journal of Banking & Finance*, 40, 80-96.

Bouslah, K., Kryzanowski, L., & M'Zali, B. (2018). Social performance and firm risk: Impact of the financial crisis. *Journal of Business Ethics*, 149(3), 643-669.

Bozanic, Z., Dietrich, J. R., & Johnson, B. A. (2017). SEC comment letters and firm disclosure. *Journal of Accounting and Public Policy*, 36(5), 337-357.

Busch, P., & Obernberger, S. (2017). Actual share repurchases, price efficiency, and the information content of stock prices. *The Review of Financial Studies*, 30(1), 324-362.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer security*, 11(3), 431-448.

Carcello, J. V., Hollingsworth, C., & Mastrolia, S. A. (2011). The effect of PCAOB inspections on Big 4 audit quality. *Research in Accounting Regulation*, 23(2), 85-96.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 70-104.

Chan, K., Hameed, A., & Kang, W. (2013). Stock price synchronicity and liquidity. *Journal of Financial Markets*, 16(3), 414-438.

Chan, K., & Chan, Y. C. (2014). Price informativeness and stock return synchronicity: Evidence from the pricing of seasoned equity offerings. *Journal of Financial Economics*, 114(1), 36-53.

Chan, K., & Hameed, A. (2006). Stock price synchronicity and analyst coverage in emerging markets. *Journal of Financial Economics*, 80(1), 115-147.

Chang, E. C., Lin, T. C., & Ma, X. (2015). The Tradeoff between Risk Sharing and Information Production in Financial Markets: Evidence from Stock Splits. Available at SSRN 2661293.

Cheema-Fox, A., LaPerla, B. R., Wang, H. S., & Serafeim, G. (2021). Corporate resilience and response to COVID-19. *Journal of Applied Corporate Finance*, 33(2), 24-40.

Cheng, L. T., Leung, T. Y., & Yu, W. (2014). Information arrival, changes in R-square and pricing asymmetry of corporate news. *International Review of Economics & Finance*, 33, 67-81.

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis*, 65, 101386.

Cornett, M. M., Erhemjamts, O., & Tehranian, H. (2016). Greed or good deeds: An

examination of the relation between corporate social responsibility and the financial performance of US commercial banks around the financial crisis. *Journal of Banking & Finance*, 70, 137-159.

Dang, T. L., Dang, M., Hoang, L., Nguyen, L., & Phan, H. L. (2020). Media coverage and stock price synchronicity. *International Review of Financial Analysis*, 67, 101430.

Datta, S., Iskandar-Datta, M., & Singh, V. (2014). Opaque financial reports and R2: Revisited. *Review of Financial Economics*, 23(1), 10-17.

de La Bruslerie, H. (2018). Do share repurchase impact analysts' activity and informativeness?. *Advances in Quantitative Analysis of Finance and Accounting*, (16), 267-309.

Demers, E., Hendrikse, J., Joos, P., & Lev, B. (2021). ESG did not immunize stocks during the COVID-19 crisis, but investments in intangible assets did. *Journal of Business Finance & Accounting*, 48(3-4), 433-462.

Ding, W., Levine, R., Lin, C., & Xie, W. (2021). Corporate immunity to the COVID-19 pandemic. *Journal of Financial Economics*, 141(2), 802-830.

Durnev, A., Morck, R., Yeung, B., & Zarowin, P. (2003). Does greater firm-specific return variation mean more or less informed stock pricing?. *Journal of Accounting Research*, 41(5), 797-836.

Durnev, A., Morck, R., & Yeung, B. (2004). Value-enhancing capital budgeting and firm-specific stock return variation. *The Journal of Finance*, 59(1), 65-105.

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

Fung, S. Y. K., Raman, K. K., & Zhu, X. K. (2017). Does the PCAOB international inspection program improve audit quality for non-US-listed foreign clients?. *Journal of Accounting and Economics*, 64(1), 15-36.

Gardberg, N. A., & Fombrun, C. J. (2006). Corporate citizenship: Creating intangible assets across institutional environments. *Academy of Management Review*, 31(2), 329-346.

Gassen, J., Skaife, H. A., & Veenman, D. (2020). Illiquidity and the measurement of stock price synchronicity. *Contemporary Accounting Research*, 37(1), 419-456.

Godfrey, P. C. (2005). The relationship between corporate philanthropy and shareholder wealth: A risk management perspective. *Academy of Management Review*, 30(4), 777-798.

Godfrey, P. C., Merrill, C. B., & Hansen, J. M. (2009). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. *Strategic Management Journal*, 30(4), 425-445.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach

announcements on firm values. *Information & Management*, 46(7), 404-410.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34, 567-594.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, 19(1), 33-56.

Gul, F. A., Kim, J. B., & Qiu, A. A. (2010). Ownership concentration, foreign shareholding, audit quality, and stock price synchronicity: Evidence from China. *Journal of Financial Economics*, 95(3), 425-442.

Haggard, K. S., Martin, X., & Pereira, R. (2008). Does voluntary disclosure improve stock price informativeness?. *Financial Management*, 37(4), 747-768.

He, Z., HuangFu, J., & Walton, S. (2022). Cybersecurity Breaches in the Supply Chain and Earnings Management. *Journal of Information Systems*, 36(3), 83-113.

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, 34(2), 187-209.

Heninger, W. G., Johnson, E. N., & Kuhn, J. R. (2018). The association between IT material weaknesses and earnings management. *Journal of Information Systems*, 32(3), 53-64.

Hogan, K. M., Olson, G. T., Mills, J. D., & Zaleski, P. A. (2023). An Analysis of Cyber Breaches and Effects on Shareholder Wealth. *International Journal of the Economics of Business*, 30(1), 51-78.

Humphrey, J. E., Lee, D. D., & Shen, Y. (2012). Does it cost to be sustainable?. *Journal of Corporate Finance*, 18(3), 626-639.

Hung, C. C., Huang, C. K., & Ku, C. Y. (2018). Research on Abnormal Return of Enterprise Stock Price for the Information Security News. *Journal of Information Management*, 25(3), 283-306.

Hutton, A. P., Marcus, A. J., & Tehranian, H. (2009). Opaque financial reports, R2, and crash risk. *Journal of Financial Economics*, 94(1), 67-86.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82(2), 85-105.

Jin, L., & Myers, S. C. (2006). R2 around the world: New theory and new tests. *Journal of Financial Economics*, 79(2), 257-292.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 12(1), 69-91.

Kothari, S. P., Leone, A. J., & Wasley, C. E. (2005). Performance matched discretionary accrual measures. *Journal of Accounting and Economics*, 39(1), 163-197.

Kvochko, E., & Pant, R. (2015). Why data breaches don't hurt stock prices. *Harvard Business Review*, March 31.

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies?. *Auditing: A Journal of Practice & Theory*, 37(1), 139-165.

Lee, C. W. J., Li, L. Y., & Yue, H. (2006). Performance, growth and earnings management. *Review of Accounting Studies*, 11(2), 305-334.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, 39(1), 151-171.

Lins, K. V., Servaes, H., & Tamayo, A. (2017). Social capital, trust, and firm performance: The value of corporate social responsibility during the financial crisis. *The Journal of Finance*, 72(4), 1785-1824.

Liu, H., & Hou, C. (2019). Does trade credit alleviate stock price synchronicity? Evidence from China. *International Review of Economics & Finance*, 61, 141-155.

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic and Social Measurement*, 43(1-2), 59-83.

Manchiraju, H., & Rajgopal, S. (2017). Does corporate social responsibility (CSR) create shareholder value? Evidence from the Indian Companies Act 2013. *Journal of Accounting Research*, 55(5), 1257-1300.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.

Morck, R., Yeung, B., & Yu, W. (2000). The information content of stock markets: why do emerging markets have synchronous stock price movements?. *Journal of Financial Economics*, 58(1-2), 215-260.

Piotroski, J. D., & Roulstone, D. T. (2004). The influence of analysts, institutional investors, and insiders on the incorporation of market, industry, and firm-specific information into stock prices. *The Accounting Review*, 79(4), 1119-1151.

Qiu, B., Yu, J., & Zhang, K. (2020). Trust and stock price synchronicity: Evidence from China. *Journal of Business Ethics*, 167(1), 97-109.

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, 33(3), 227-265.

Roll, R. (1988). R^2. *Journal of Finance*, 43(3), 541-566.

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.

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3), 701-728.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974.

Shiu, Y. M., & Yang, S. L. (2017). Does engagement in corporate social responsibility provide strategic insurance-like effects?. *Strategic Management Journal*, 38(2), 455-470.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229.

Stoel, M. D., & Muhanna, W. A. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems*, 12(4), 280-304.

Ting, H. I., & Huang, Y. T. (2010). The Impact of Information Disclosure Level and Content on the Institutional Investors' Shareholdings. *Review of Securities and Futures Markets*, 22(3), 39-74.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, 101795.

Utz, S. (2018). Over-investment or risk mitigation? Corporate social responsibility in Asia-Pacific, Europe, Japan, and the United States. *Review of Financial Economics*. 36, 167-193.

Xu, N., Chan, K. C., Jiang, X., & Yi, Z. (2013). Do star analysts know more firm-specific information? Evidence from China. *Journal of Banking & Finance*, 37(1), 89-102.

Xu, X., & Li, J. (2020). Asymmetric impacts of the policy and development of green credit on the debt financing cost and maturity of different types of enterprises in China. *Journal of Cleaner Production*, 264, 121574.

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems*, 33(3), 267-284.

Xu, L., Huang, Z. J., & Wen, F. (2022). Comment letters and stock price synchronicity: evidence from China. *Review of Quantitative Finance and Accounting*, 59(4), 1387-1421.

Zheng, S., Zhang, X., & Wang, H. (2023). Green credit policy and the stock price synchronicity of heavily polluting enterprises. *Economic Analysis and Policy*, 77, 251-264.

Table 1 Sample Description

This table illustrates the sample selection process and the distribution of individual stocks across industries in the sample. Panel A shows the sample selection process for non-financial firms (firm-years) listed on TWSE and TPEx between 2013 and 2023. Observations with missing values for control variables or without ESG data were excluded. Panel B presents the distribution of individual stocks across TEJ industry classifications, comparing firms with and without data breaches.

Panel A: Sample Selection

	Numbers of observations	Breached firm-years	Non-Breached firm-year
Non-financial firms listed in TWSE or TPEx (2013-2023)	17,410		
Less: firm-year observations with missing values to construct control variables	(1,413)		
All firms sample (H1)	15,997	532	15,465
Less: firm-year observations with missing values of ESG data	(3,903)		
H2 sample	12,094	397	11,697

Panel B: Industry Distributions

TEJ Code	Industry	Non-Breached	Breached	Total
M11	Cement	129	0	129
M12	Food Products	304	0	304
M13	Petrochemical & Rubber	355	22	377
M14	Textile & Synthetic Fiber	586	0	586
M15	Mechanical Electronics	1,065	55	1,120
M16	Electric Wire	110	0	110
M17	Chemical	1,406	50	1,456
M18	Ceramic & Glass	65	0	65
M19	Papermaking	68	0	68
M20	Iron & Steel	553	11	564
M21	Rubber & Tire	105	11	116
M22	Automobile	136	22	158
M23	Electronic	7,911	295	8,206
M25	Construction & Building	1,018	11	1,029
M26	Transportation-All	281	11	292
M27	Tourism	344	16	360
M28K	Lease/Rental	15	0	15
M29	General Merchandise	224	11	235
M99	Other	790	17	807
Total		15,465	532	15,997

Table 2 Summary Statistics

This table presents the descriptive statistics of variables for individual stocks in the sample. Panel A shows the mean, standard deviation, 25th percentile (Q1), median, and 75th percentile (Q3) for all variables, including: $SYNCH$ (stock price synchronicity), BDS (a dummy variable where 1 indicates a company experienced an information security incident, and 0 otherwise), $SIZE$ (the natural logarithm of market capitalization), MTB (the market-to-book ratio), $Leverage$ (the ratio of total liabilities to total assets), ROE (the return on equity), VOL (standard deviation of weekly industry returns), $SKEW$ (skewness of weekly returns), $KURT$ (kurtosis of weekly returns), $ZeroReturn$ (ratio of zero-return days to total trading days), and $TradeVol$ (natural logarithm of trading volume). Panel B compares the differences in these variables between firms with and without data breaches. The two rightmost columns display the results of difference tests for means medians between firms with and without data breaches. Significance levels are indicated as follows: * for p-values < 0.1, ** for p-values < 0.05, and *** for p-values < 0.01.

Panel A: All Samples (N=15,997)

Variable	Mean	Std.	Q1	Median	Q3
$SYNCH$	-1.590	1.151	-2.286	-1.467	-0.760
BDS	0.033	0.179	0.000	0.000	0.000
$SIZE$	15.105	1.373	14.120	14.908	15.909
MTB	1.900	2.395	0.833	1.268	2.040
$Leverage$	0.360	0.167	0.223	0.350	0.485
ROE	0.061	0.116	0.010	0.070	0.136
VOL	4.645	2.349	2.902	4.235	5.907
$SKEW$	0.582	0.945	-0.037	0.489	1.112
$KURT$	5.718	2.570	3.763	4.924	6.965
$ZeroReturn$	0.115	0.080	0.061	0.095	0.146
$TradeVol$	4.682	1.741	3.497	4.700	5.900

Panel B: Mean and Median Difference between Breached and Non-Breached Firms

	(1) Breached (N=532)		(2) Non-Breach (N=15,465)		Difference (1)- (2)	
Variable	Mean	Median	Mean	Median	Mean	Median
$SYNCH$	-1.257	-1.164	-1.603	-1.483	0.344***	0.31***
BDS	16.343	16.254	15.060	14.882	1.281***	1.371***
$SIZE$	1.770	1.318	1.910	1.267	-0.135	0.052
MTB	0.397	0.384	0.359	0.349	0.038***	0.035***
$Leverage$	0.081	0.093	0.060	0.069	0.021***	0.025***
ROE	4.542	4.073	4.651	4.239	-0.106	-0.165
VOL	0.429	0.298	0.587	0.496	-0.158***	-0.198***
$SKEW$	5.202	4.458	5.736	4.938	-0.534***	-0.480***
$KURT$	0.086	0.075	0.117	0.097	-0.030***	-0.022***
$ZeroReturn$	5.851	5.981	4.642	4.668	1.209***	1.318***

Table 3 Effect of Cybersecurity Incidents on Stock Price Synchronicity

This table presents the regression estimates for Hypotheses 1a and 1b, where the dependent variable is $SYNCH$ (stock price synchronicity). Both Columns (1) and (2) are based on the model specified in Equation (2). Column (1) tests the primary variables, BDS (a dummy indicating whether a company experiences a cybersecurity incident) and $BDS \times Post$ (an interaction term where $Post$ is a dummy equal to 1 after the incident 0 before), without additional controls. Column (2) incorporates control variables, including $SIZE$ (natural logarithm of market capitalization), MTB (market-to-book ratio), $Leverage$ (total liabilities to total assets ratio), ROE (return on equity), VOL (standard deviation of weekly industry returns), $SKEW$ (skewness of weekly returns), $KURT$ (kurtosis of weekly returns), $ZeroReturn$ (proportion of zero-return trading days), and $TradeVol$ (natural logarithm of trading volume). Significance levels are denoted as: * for p-values < 0.1, ** for p-values < 0.05, and *** for p-values < 0.01.

Dependent variable: SYNCH	(1)	(2)
$Intercept$	-1.681***	-2.804***
	(-80.724)	(-16.393)
BDS	0.551***	0.287***
	(7.152)	(4.011)
$BDS \times Post$	0.201**	0.142*
	(2.157)	(1.652)
$SIZE$		0.129***
		(10.776)
MTB		-0.004***
		(-4.001)
$Leverage$		-0.386***
		(-6.036)
ROE		-0.052
		(-0.647)
VOL		-0.031***
		(-6.954)
$SKEW$		-0.305***
		(-34.690)
$KURT$		0.007**
		(2.182)
$ZeroReturn$		-2.518***
		(-18.317)
$TradeVol$		-0.016*
		(-1.763)
Year fixed effect	Yes	Yes
Industry fixed effect	Yes	Yes
Firm fixed effect	Yes	Yes
N	15,997	15,997
adj. R^2	0.305	0.415

Table 4 Effect of Cybersecurity Incidents on Stock Price Synchronicity: The Moderating Effect of ESG

This table presents the regression estimates for Hypotheses 2, where the dependent variable is $SYNCH$ (stock price synchronicity). Both Columns (1) and (2) are based on the model specified in Equation (3), where the primary variables include BDS (a dummy indicating whether a company experiences a cybersecurity incident) and $BDS \times Post$ (an interaction term where $Post$ is a dummy equal to 1 after the incident 0 before). In Column (1), ESG scores are categorized into two groups based on the industry median, with a dummy variable ($HighESG$) assigned as 1 if a company's ESG score is above the median, and 0 otherwise. In Column (2), ESG is treated as a continuous score (ranging from 0 to 100). Control variables include $SIZE$ (natural logarithm of market capitalization), MTB (market-to-book ratio), $Leverage$ (total liabilities to total assets ratio), ROE (return on equity), VOL (standard deviation of weekly industry returns), $SKEW$ (skewness of weekly returns), $KURT$ (kurtosis of weekly returns), $ZeroReturn$ (proportion of zero-return trading days), and $TradeVol$ (natural logarithm of trading volume). Significance levels are denoted as: * for p-values < 0.1, ** for p-values < 0.05, and *** for p-values < 0.01.

Dependent variable: SYNCH	(1)	(2)
$Intercept$	-1.822***	-1.821***
	(-7.608)	(-7.531)
BDS	-0.185	-0.093
	(-1.099)	(-0.155)
$BDS \times Post$	0.255*	1.095*
	(1.905)	(1.956)
$BDS \times HighESG$	0.130	-0.001
	(0.911)	(-0.085)
$BDS \times Post \times HighESG$	-0.306*	-0.017*
	(-1.826)	(-1.837)
$HighESG$	0.009	-0.001
	(0.443)	(-0.710)
$SIZE$	0.075***	0.079***
	(4.633)	(4.827)
MTB	-0.001	-0.001
	(-1.335)	(-1.354)
$Leverage$	-0.136*	-0.135*
	(-1.683)	(-1.676)
ROE	0.066	0.068
	(0.714)	(0.739)
VOL	-0.029***	-0.030***
	(-5.695)	(-5.782)
$SKEW$	-0.261***	-0.261***
	(-29.141)	(-29.166)
$KURT$	-0.001	-0.000
	(-0.179)	(-0.128)
$ZeroReturn$	-3.036***	-3.036***
	(-16.249)	(-16.248)
$TradeVol$	-0.058***	-0.058***
	(-5.243)	(-5.239)
Year fixed effect	Yes	Yes
Industry fixed effect	Yes	Yes
Firm fixed effect	Yes	Yes
N	12,094	12,094
adj. R^2	0.472	0.472

Table 5 Effect of Cybersecurity Incidents on Stock Price Synchronicity: Considering the Role of CISO

This table examines whether the presence of a CISO influences the extent to which cybersecurity incidents affect stock price synchronicity. The dependent variable is $SYNCH$ (stock price synchronicity). BDS is a dummy indicating whether a company experiences a cybersecurity incident, and $BDS \times Post$ is an interaction term where $Post$ is a dummy equal to 1 after the incident 0 before. Control variables include $SIZE$ (natural logarithm of market capitalization), MTB (market-to-book ratio), $Leverage$ (total liabilities to total assets ratio), ROE (return on equity), VOL (standard deviation of weekly industry returns), $SKEW$ (skewness of weekly returns), $KURT$ (kurtosis of weekly returns), $ZeroReturn$ (proportion of zero-return trading days), and $TradeVol$ (natural logarithm of trading volume). Significance levels are denoted as: * for p-values < 0.1, ** for p-values < 0.05, and *** for p-values < 0.01.

Dependent variable: $SYNCH$	
$Intercept$	-2.097***
	(-13.213)
BDS	0.347***
	(4.955)
$BDS \times Post$	0.182**
	(2.144)
$BDS \times CISO$	0.462
	(0.887)
$BDS \times Post \times CISO$	-0.937*
	(-1.740)
$CISO$	0.175***
	(3.839)
$SIZE$	0.086***
	(7.766)
MTB	-0.003***
	(-3.401)
$Leverage$	-0.401***
	(-6.999)
ROE	-0.080
	(-1.114)
VOL	-0.033***
	(-8.099)
$SKEW$	-0.260***
	(-33.405)
$KURT$	0.004
	(1.420)
$ZeroReturn$	-3.038***
	(-19.764)
$TradeVol$	-0.023***
	(-2.641)
Year fixed effect	Yes
Industry fixed effect	Yes
Firm fixed effect	Yes
N	15,997
adj. R^2	0.425

Table 6 Effect of Cybersecurity Incidents on Stock Price Synchronicity: Considering the Role of Earnings Quality

This table examines whether earnings quality influences the effect of cybersecurity incidents on stock price synchronicity. The dependent variable is $SYNCH$ (stock price synchronicity). The key variables include BDS (a dummy indicating whether a company experiences a cybersecurity incident) and $BDS \times Post$ (an interaction term where $Post$ is a dummy equal to 1 after the incident 0 before). FRQ is a financial reporting quality dummy variable. If the absolute value of a company's discretionary accruals ($ABSDA$, defined in Equation (5)) is below the industry median for the year, FRQ is set to 1, indicating lower earnings management and implying better earnings quality. If the $ABSDA$ is greater than or equal to the industry median for the year, FRQ is set to 0, indicating poorer earnings quality. Control variables include $SIZE$ (natural logarithm of market capitalization), MTB (market-to-book ratio), $Leverage$ (total liabilities to total assets ratio), ROE (return on equity), VOL (standard deviation of weekly industry returns), $SKEW$ (skewness of weekly returns), $KURT$ (kurtosis of weekly returns), $ZeroReturn$ (proportion of zero-return trading days), and $TradeVol$ (natural logarithm of trading volume). Significance levels are denoted as: * for p-values < 0.1, ** for p-values < 0.05, and *** for p-values < 0.01.

Dependent variable: $SYNCH$	
$Intercept$	-1.737***
	(-12.649)
BDS	0.245***
	(3.315)
$BDS \times Post$	0.066
	(0.603)
$BDS \times FRQ$	-0.007
	(-0.100)
$BDS \times Post \times FRQ$	-0.245*
	(-1.670)
FRQ	0.022*
	(1.766)
$SIZE$	0.049***
	(4.918)
MTB	-0.002***
	(-2.885)
$Leverage$	-0.426***
	(-8.397)
ROE	0.062
	(0.942)
VOL	-0.048***
	(-12.474)
$SKEW$	-0.247***
	(-32.483)
$KURT$	0.008***
	(2.852)
$ZeroReturn$	-2.697***
	(-18.723)
$TradeVol$	-0.001
	(-0.078)
Year fixed effect	Yes
Industry fixed effect	Yes
Firm fixed effect	Yes
N	15,997
adj. R^2	0.451

Table 7 Effect of Cybersecurity Incidents on Stock Price Synchronicity: Controlling for Endogeneity Factors (Propensity-score Matching)

This table presents the re-estimation of parameters for testing Hypotheses 1 and 2, using propensity-score matching to control for factors that may influence the likelihood of a company experiencing a cybersecurity incident. In Panel A, Column (1) displays the re-estimated results for Equation (2). Columns (2) and (3) provide the re-estimated results for Equation (3). Specifically, in Column (2), ESG scores are categorized into two groups based on the industry median, with a dummy variable ($HighESG$) assigned a value of 1 if a company's ESG score is above the median, and 0 otherwise. In Column (3), ESG is treated as a continuous score ranging from 0 to 100. Panel B presents the re-estimated regression results considering the presence or absence of a CISO (in Column (1)) and the quality of earnings (in Column (2)). Significance levels are denoted as: * for p-values < 0.1, ** for p-values < 0.05, and *** for p-values < 0.01.

Panel A: Re-estimation of Parameters for Testing Hypotheses 1 and 2 (Matched Sample)

Dependent variable: SYNCH	(1)	(2)	(3)
$Intercept$	-5.117***	-4.002***	-3.668***
	(-6.647)	(-4.261)	(-3.419)
BDS	0.549***	0.301	-0.742
	(3.292)	(1.396)	(-0.948)
$BDS{\times}Post$	0.205**	0.261*	1.224**
	(1.967)	(1.780)	(2.096)
$BDS{\times}HighESG$		0.157	0.020
		(0.709)	(1.419)
$BDS{\times}Post{\times}HighESG$		-0.384**	-0.020**
		(-2.017)	(-2.046)
$HighESG$		0.098	-0.003
		(0.663)	(-0.255)
$SIZE$	0.250***	0.208***	0.199***
	(5.445)	(3.665)	(3.191)
MTB	-0.072***	-0.070***	-0.068***
	(-3.779)	(-2.950)	(-2.837)
$Leverage$	0.418*	0.046	0.079
	(1.677)	(0.152)	(0.265)
ROE	-1.371***	-1.130**	-1.103**
	(-3.118)	(-2.090)	(-2.057)
VOL	-0.034	-0.022	-0.023
	(-1.538)	(-0.845)	(-0.868)
$SKEW$	-0.324***	-0.281***	-0.281***
	(-8.189)	(-6.189)	(-6.184)
$KURT$	0.009	-0.007	-0.006
	(0.613)	(-0.406)	(-0.393)
$ZeroReturn$	-4.497***	-3.504***	-3.529***
	(-5.172)	(-3.427)	(-3.451)
$TradeVol$	-0.001***	-0.002***	-0.002***
	(-3.912)	(-3.592)	(-3.562)
Year fixed effect	Yes	Yes	Yes
Industry fixed effect	Yes	Yes	Yes
Firm fixed effect	Yes	Yes	Yes
N	1,028	770	770
adj. R^2	0.468	0.500	0.500

Panel B: Re-estimation of Parameters Considering the Role of CISO and Earnings Quality		
Dependent variable: SYNCH	(1)	(2)
$Intercept$	-3.230***	-2.284***
	(-5.088)	(-3.665)
BDS	0.387***	0.537***
	(3.541)	(4.161)
$BDS \times Post$	0.310***	0.141
	(2.703)	(1.242)
$BDS \times CISO$	0.482	
	(0.736)	
$BDS \times Post \times CISO$	-1.276**	
	(-1.974)	
$CISO$	0.240	
	(1.088)	
$BDS \times FRQ$		0.022
		(0.224)
$BDS \times Post \times FRQ$		-0.293**
		(-2.080)
FRQ		0.021
		(0.303)
$SIZE$	0.139***	0.093***
	(3.923)	(2.712)
MTB	-0.061***	-0.040***
	(-3.257)	(-2.672)
$Leverage$	0.149	-0.062
	(0.634)	(-0.287)
ROE	-0.636	-0.883***
	(-1.483)	(-2.592)
VOL	-0.044**	-0.034**
	(-2.106)	(-1.999)
$SKEW$	-0.338***	-0.232***
	(-8.350)	(-7.414)
$KURT$	0.015	-0.002
	(1.008)	(-0.175)
$ZeroReturn$	-5.610***	-3.381***
	(-6.633)	(-5.029)
$TradeVol$	-0.001***	-0.001***
	(-2.651)	(-3.623)
Year fixed effect	Yes	Yes
Industry fixed effect	Yes	Yes
Firm fixed effect	Yes	Yes
N	1,028	1,028
adj. R^2	0.449	0.497

Appendix 1 Variable Definitions

Variable	Definition
$SYNCH$	stock price synchronicity. $SYNCH_{it} = \ln\left(\frac{R_{it}^2}{1-R_{it}^2}\right)$, the R^2 estimated from Equation (1).
BDS	1 if a firm has a cybersecurity incident in year t, 0 otherwise.
$Post$	1 if a fiscal year is after a cybersecurity incident.
$SIZE$	The natural logarithm of market value.
MTB	The ratio of the market value of equity to the book value of equity at the end of last fiscal year.
$Leverage$	Total liabilities divided by total assets.
ROE	The contemporaneous income before extraordinary items divided by the book value of equity.
VOL	The standard deviation of weekly industry returns over the fiscal year.
$SKEW$	The skewness of firm-specific weekly return over the fiscal year.
$KURT$	The kurtosis of firm-specific weekly return over the fiscal year.
$ZeroReturn$	The fraction of zero-return days in a firm-year.
$TradeVol$	The natural logarithm of trade volume.
$HighESG$	ESG data is primarily sourced from the TEJ. ESG scores are based on three dimensions: environmental, social, and governance. Scores for each dimension are calculated using relative rankings that range from 0 to 100. Higher scores indicate better ESG performance. If the ESG score is greater than the median, $HighESG$ is equal to 1, otherwise it is 0.