Information Systems Frontiers
https://doi.org/10.1007/s10796-025-10639-6

The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study

Dewan Muktadir-Al-Mukit[1] · **Md Hakim Ali**[2]

Received: 16 September 2024 / Accepted: 6 August 2025

Abstract
With the growing digital integration of business operations, cybersecurity risks have also increased significantly, posing a potential threat to stock prices through increased volatility. Our study investigates the impact of cyber-attacks on the stock prices of US listed firms, using a dataset of 776 incidents between 2012 and 2022. We argue that although cyber-attacks typically trigger negative stock market responses, the extent and nature of this reaction depend on several key factors, including the source and credibility of the news, the incident's severity and distinctiveness, data privacy concerns, and the industry's overall exposure to cyber risks. Our event study shows that firms lose $309.33 million in market value on the day a cyber-attack is reported. We observe that the negative response intensifies when cyber-attack news emerges in influential sources, indicating a wider media coverage and source credibility effect. We find that the negative reaction is more pronounced when the cyber-attack has a high consequential effect (severity). Moreover, firms that confront cyber-attacks for the first-time face overreaction from investors and greater losses than those with consecutive cyber-attacks. Sub-period analysis focusing on the 2015 Office of Personnel Management (OPM) data breach and the COVID-19 era shows more pronounced stock price impacts during the post-OPM and pre-COVID periods. Cross-sectional findings also reveal that firms with higher societal expectations for data privacy and those operating in sectors more vulnerable to cyber threats experience more negative reactions. Hence, our study provides insights for policymakers, regulators, and corporate leaders on cyber breach disclosure, transparency, timeliness and cybersecurity governance to strengthen market stability, corporate resilience, and investor confidence.

Keywords Cyber-attack · News coverage · Data privacy · Cyber resilience · Shareholder value · Cumulative abnormal return

JEL Classifications G11 · G14 · G32 · G41

1 Introduction

With the advancement of technology, firms are increasingly becoming digitalized. This technological advancement brings both benefits and drawbacks. On the downside, one of the striking issues is the risk of cyber-attacks, which have become a common phenomenon across companies and industries throughout the world. Even more alarming is the fact that cyber breach incidents and damages are rising steadily across the world.[1] These breaches not only disrupt business operations but also causes significant financial

✉ Dewan Muktadir-Al-Mukit
D.Mukit@shu.ac.uk

Md Hakim Ali
h.ali@mmu.ac.uk

[1] Finance and Economics Division, Sheffield Business School, Sheffield Hallam University, Howard Street, Sheffield S1 1WB, UK

[2] Department of Finance and Economics, Faculty of Business and Law, Manchester Metropolitan University, Manchester M15 6BX, UK

[1] See CyberEdge: Cyberthreat Defense Report, pg 21. https://cyberedgegroup.com/wp-content/uploads/2023/10/CyberEdge-2023-CDR-Report-v1.0.pdf.

Published online: 16 October 2025

losses for the affected firm. The recent data[2] on the cost of cybersecurity risk show that the global average cost of cyber breach was USD 4.88 million in 2024, a 10% increase from 2023 and highest since the pandemic. The predicted cost of cybercrime for global economy was USD 9.4 trillion in 2024,[3] with an expected increase of 15% in 2025. Moreover, companies that experience cyber-attacks often find themselves in a challenging position to survive. To this end, the National Cybersecurity Alliance estimates that 60% of small business shut down their business within six months of cyber-attacks. This highlights the serious threat to the long-term viability of businesses targeted by cyber attacks. Considering the value implications of cybersecurity risk, investors are concerned about firms' performance (Spanos & Angelis, 2016; Tosun, 2021); internal controls weakness (Zhou & Huang, 2024) and additional cybersecurity investment (Shaikh & Siponen, 2024).

Although the costs of a security breach at the firm level are diverse including financial loss, data loss, recovery costs, repair expenses, and reputational damage, we focus on the movement of stock returns around the security breach event as part of a post-event analysis in light of the stock market response. This is particularly relevant, as the growing investor focus on cybersecurity risk has had a significant impact on companies and their stakeholders (Jiang et al., 2024; Walton et al., 2021). A cybersecurity breach can be costly due to revenue loss, declining profitability and stock prices, and subsequent legal expenses (Gordon et al., 2011; Jeong et al., 2019; Huang & Wang, 2021). This highlights the rising significance of cyber threats in financial decision-making. As the frequency and complexity of cyber-attacks continue to grow, investors around the world are paying closer attention to their financial and operational implications. This heightened awareness emphasizes the need for a thorough evaluation of how cyber vulnerabilities influence firm valuation, investor confidence, and long-term business resilience.

Our study is based on the concept of the animal spirits notion, which suggests that investors' emotions drive financial decision-making in uncertain environments and volatile times (Lansing, 2019). Moreover, the market psychology perspective implies that stock prices respond to both positive and negative events occurring within firms. It is evident that cybersecurity is now regarded as one of the most critical business risks, also classified as a form of systematic risk that can potentially escalate into a black swan event, causing immense losses to firms and the broader economy. Therefore, it is important to assess whether market participants respond immediately to cybersecurity risks. The response pattern may vary depending on assumptions about the breach. For example, investors may suspect loopholes in the cybersecurity system, weak infrastructure, underreported damages, the likelihood of repeated breaches, and reputational loss. Additionally, market reactions can differ based on the timing of the incident, the spread and depth of the news, and the accessibility and availability of news platforms. Therefore, in this study, we explore how cyber-attack news affects investment decisions in the stock market. Specifically, we examine stock price reactions to cyber-attack disclosures and whether these reactions depend on news variability, event intensity, and specific firm characteristics.

According to the Efficient Market Hypothesis (EMH), financial markets efficiently process information, leading to rapid price adjustments based on publicly available data. Empirical evidence supports this view, demonstrating that stock prices incorporate new information, including cybersecurity incidents (Florackis et al., 2023). A notable characteristic of the stock market is that return volatility fluctuates based on the spread, intensity, and availability of negative news; we assume the same applies to cyber events. The existing literature presents two main perspectives regarding the impact of cyber-attacks on stock prices. One group of scholars argues that cyber breaches directly affect stock prices (Amir et al., 2018; Tosun, 2021), while another group contends that such breaches primarily increase market volatility (Jamilov et al., 2023). Hence, previous research on the relationship between cyber incidents and stock price behavior remains inconclusive, prompting the need for further investigation.

Several factors may explain these mixed findings. First, market efficiency determines how quickly cyber-attack news spreads and influences investor decisions. Second, in some markets, investors may have already priced in cybersecurity risks, leading to minimal stock price impact (Foecking et al., 2021). Third, increasing awareness and acceptance of cybersecurity threats may have made investors more resilient, recognizing that no security system is entirely immune to attacks (McShane & Nguyen, 2020). Finally, risk management initiatives may also affect the relationship between cyber incidents and stock prices. For example, Kamiya et al. (2021) reveal that a successful cyber-attack reduces the stock price, and this effect is lower when there is a proactive risk management by the board, and it becomes more severe if the attack decreases sales growth. In the event of a cyber breach, a firm's reputation will suffer because they are not able to meet stakeholders' expectations of strong cybersecurity risk management. Consequently, the spread of this

[2] The cost of a data breach report 2023 prepared by IBM Security is available here: https://www.ibm.com/reports/data-breach.

This average cost is based on data from 604 organizations affected by breaches between March 2023 and February 2024 across 16 countries.

[3] The information on cybercrime cost can be accessed here: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/.

news or information can cast doubt on the credibility and resilience of the affected firm. Therefore, it is imperative to test the market reaction hypothesis following a cyber-attack, as operational risk affects stock market performance (Bai et al., 2021).

In this study, we use a sample of US listed firms that experienced cyber-attacks between 2012 and 2022. We get cyber-attack data from RepRisk, a prominent database for business conduct risk.[4] We study the US market since this is characterized as highly elastic and volatile where share price responds to any relevant information available. Moreover, US is one of the most vulnerable countries to cyber-attack.[5] According to IT governance, the US is found to suffer more publicly disclosed incidents than any other country in the world.[6] Moreover, nearly every sector is affected by cyber-attacks in the US market.[7] Besides, the market reaction hypothesis asserts that share price value is influenced by strong cyber risk management in the era of digitalization, which is also aligned with the US cybersecurity act 2011. Therefore, the news of the cyber breach incidents provides an opportunity to test whether media coverage of cyber breaches had an observable effect on the share prices of US public firms that experienced a cyber-attack.

We conduct an event study to examine the impact of cyber-attack news on stock prices. Our findings indicate that, on average, firms experience a $309.33 million loss on the day a cyber breach is reported, suggesting that investors penalize companies when their security systems are compromised. This market penalty intensifies over a three-day event window, with cumulative losses reaching $618.65 million, highlighting that investors actively adjust their trading decisions in response to cyber-attacks. We further analyse the role of news media in disseminating breach information. Our results suggest that cyber-attacks covered by major media platforms such as Financial Times and CNN amplify stock price declines, as these platforms provide wider investor access and greater market influence. The credibility and reach of news sources significantly affect stock performance, as widely trusted media disseminate information more rapidly than smaller and less reputable platforms. This aligns with findings that heightened investor concerns over data breaches contribute to stock price crashes (Cao et al., 2024). We then examine stock price reactions based on attack severity and find that more severe cyber-attacks lead to stronger negative responses. Finally, our analysis reveals that first-time cyber-attacks trigger greater losses than repeated breaches, likely due to policy restructuring and management changes, which help restore investor confidence after an initial breach.

We further explore the effect of cyber breaches before and after the Office of Personnel Management (OPM) data breach in 2015. This event is significant, as it marked one of the largest cyber incidents in the US history, compromising 22.1 million records. We find that the effect on stock returns is more pronounced after the OPM incident. This may be attributed to the severe consequences of cyber-attacks and growing awareness of such threats. We also examine a pre- and post-COVID-19 analysis, which shows that stock market reactions were more pronounced in the pre-COVID-19 period. In addition, using cross-sectional analysis, we find that negative stock price reactions to cyber-attack news are larger for firms with more robust data privacy systems, implying that investor trust is particularly eroded when highly secure systems are breached. Moreover, we find more pronounced stock price reactions in specific sectors, such as financials, energy, and retail.

Our study makes significant contributions to the cybersecurity risk and finance literature by expanding on the value relevance of cybersecurity breaches. Prior research has examined the financial costs of security breaches (Aldasoro et al., 2022; Eling & Wirfs, 2019; Tao et al., 2019) and their impact on stock prices (Campbell et al., 2003; Goel & Shawky, 2009; Kamiya et al., 2021; Tosun, 2021; Tripathi & Mukhopadhyay, 2020). These studies report varying stock price declines based on breach characteristics and timeframes. However, our study supplements these prior studies by exploring how investors react to cyber-attack incidents when reported in news media. Our sample is significantly larger and covers a more recent time period, making it substantially greater in scale compared to previous studies. Notably, our cyber-attack news is obtained from RepRisk, which uses artificial intelligence (AI) and natural language processing to track incident news,[8] thus reducing selection bias and increasing the generalizability of our results.

Second, unlike any prior studies, we contribute by showing whether investor reactions depend on media source influence, incident severity, and novelty. We for the first time examine the news media effect while there is a cyber-attack. We uncover that the heterogeneity in popularity of news platform that report cyber breach has varying effect

[4] See https://www.forbes.com/sites/ankitmishra/2022/02/14/reprisks-risk-platform-aims-to-bring-transparency-into-esg-corporate-reporting/.

[5] Read this article on most vulnerable countries to cyberattack here: https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/.

[6] See the recent statistics of cyber-attack in the USA here: https://www.itgovernanceusa.com/blog/data-breaches-and-cyber-attacks-in-the-usa-in-april-2024-4277728098-records-breached.

[7] For example, a recent cyber-attack in the health care shut down the health care payment system. For more details read this article to explore the healthcare vulnerability to cyber-attack: https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

[8] See https://www.reprisk.com/news-research/resources/the-advantage-of-artificial-human-intelligence-at-reprisk.

on investors' response. By estimating news media effect, we provide important insights towards stock trading decision around the cyber event. Moreover, we also show that the stock price reaction depends on the consequential effects of the data breach as well as the newness of the incident.

Third, we contribute to the literature on learning how rising awareness on cyber-attack affect the investors' response towards news on cyber breach. We uncover that the cybersecurity awareness following major data breach event like OPM results more pronounced market reaction. Moreover, our findings show that the COVID-19 pandemic influences the risk perception of cyber-attack which implies that the investors' response during pre and post COVID-19 are not the same. Finally, our study also provides cross-sectional evidence on how investors value data privacy policy and sectoral impact following cyber-attack news.

The rest of the paper is structured as follows. Section 2 includes the hypothesis development supported by the underlying theoretical discussion. Section 3 outlines the data and sample selection along with a description of methodology. Section 4 shows the findings including cross-sectional and robustness analysis, Section 5 shows discussion and Section 6 provides concluding remarks with practical implication and future research direction.

2 Hypothesis Development

There is a large literature on stock market reaction to the corporate events. The market reaction can reflect in weaker, positive or even negative reaction depending on the nature and magnitude of the event. Earlier studies shed light on market reaction to the information of different events, such as the corporate governance (Carlini et al., 2020), corporate illegalities (Davidson et al., 1994; Song & Han, 2017), corporate earnings announcement (Cready & Gurun, 2010; Pevzner et al., 2015) and corporate social responsibility (Flammer, 2013; Krüger, 2015; Su et al., 2016). However, only a limited number of studies exploring the cyber-attack and stock market reaction (Cavusoglu et al., 2004; Goel & Shawky, 2009; Tripathi & Mukhopadhyay, 2020; Kamiya et al., 2021; Tosun, 2021; Martins & Moutinho, 2025). These studies show that cyber-attacks have impact on the stock prices of the affected firms. Specifically, investors negatively value firms associated with cyber breaches. Nevertheless, earlier research has not adequately addressed the role of the media in spreading news about cyber-attacks that affect firm's stock price. This is important as security has been a serious concern in this digitalized and globalized world. Given the rise of cyber-attacks and the diversity of associated factors, cybersecurity risk has become a serious issue that needs to be widely explored from the investor's perspective. Among other objectives, one purpose of cyber event reporting is to provide investors with information of cyber-attack that they can use to evaluate their investment decisions. Moreover, regulatory bodies and industry players also regularly express concern over the cyber-attack.[9]

Any cyber-attack has significant impact on operations, reputation, and financial stability of portfolio firms (Corbet & Gurdgiev, 2019; Kamiya et al., 2021). The affected firm may suffer financially from cyber-attacks due to business disruption, physical damages and theft of intellectual property, impacting borrowing capacity by lowering credit ratings and increasing the need for heavy borrowing to recover. Moreover, affected firms may suffer from a loss of sales revenue due to eroding customer trust, which also takes significant time to rebuild.[10] Firms may additionally incur loss from regulatory fines and legal settlement for data breach (Romanosky et al., 2014). Therefore, reported cyber-attack news is likely to have notable impact on the stock market, which is expected to be negative, as we argue that the widespread loss and severe consequences of a cyber-attack will create a 'fear of missing out' sentiment among investors. Alternatively, market participants seek to avoid the loss of stock returns immediately after news of a cyber-attack. Therefore, investors are likely to pay attention to news of a firm's cybersecurity breach and react strongly to information about the cyber-attack. Hence, the extent and speed of the market reaction depend on factors such as market transparency, information dissemination, and investor attention. Given the assumptions of a semi-strong form efficient market, where information is relatively reflected in prices at faster speed, we expect cyber-attack news to have a negative effect on stock returns. Based on this reasoning, we propose the following hypothesis:

H_1: Stock market reacts negatively to the corporate cyber-attacks news in the short run.

Investor responses to corporate events are shaped not only by the events themselves but also by how the information is presented. Media plays a crucial role in shaping narratives and influencing market sentiment. It can significantly affect investor awareness and attention (Kölbel et al., 2017; Barkemeyer et al., 2020; Carlini et al., 2020; Hao & Xiong,

[9] See https://www.thomsonreuters.com/en-us/posts/government/sec-cybersecurity-rules/.

See https://www.gov.uk/government/news/business-leaders-urged-to-toughen-up-cyber-attack-protections.

[10] See https://vercara.com/news/vercara-research-75-of-u-s-consumers-would-stop-purchasing-from-a-brand-if-it-suffered-a-cyber-incident.

See Global Security Research report (2024): Extracted from https://learn.fastly.com/the-race-to-adapt.

2021), often amplifying perceptions and biases, particularly for firms in the public spotlight (Hillert et al., 2014). Since investors rely on media for timely information (Tetlock, 2007), firms receiving media attention are more exposed to negative coverage, which can adversely impact their stock prices (Wu & Lin, 2017). Although cyber-attacks represent a growing systemic risk, limited awareness and detection difficulties often hinder investors' ability to assess such risk. However, when such incidents are reported by reputable outlets such as Financial Times or CNN, investor attention is likely to increase due to higher perceived credibility (Pornpitakpan, 2004; Rhee & Fiss, 2014). In contrast, coverage by less credible or local media may fail to trigger a strong market reaction. Therefore, we anticipate that cyber-attacks reported by influential media will lead to more severe stock market penalties for the affected firms.

Stock price reaction may also depend on the seriousness/severity of the cyber-attack incident. Previous studies report the variation of the effect on stock market with severity and magnitude of the incident (Kaplanski & Levy, 2010). For example, Capelle-Blancard and Laguna (2010) find that 64 explosions in chemical plants and refineries worldwide over the period 1990–2005 caused average stock price declines of 0.76% on the event day and 1.26% on the following day for the affected firms. Hence, it is more likely that abnormal return loss is high when the severity of the incident is in higher magnitude. Cyber-attack with serious loss and more consequential effect is likely to affect the stock market more negatively than those are less severe. This is because the negative effect of cyber-attacks is likely to be amplified as the level of psychological effect increases due to the sentiment effect of greater loss of cyber-attacks.

We also argue that a subsequent cyber-attack on the same firm may have a different impact on its stock price, as investor sentiment, trust, and confidence may shift after the initial incident. Firms typically respond to cyber-attacks by restructuring corporate governance and risk management policies (Lending et al., 2018; Nordlund, 2019). For example, Equifax's CEO Richard Smith and other executives resigned following a data breach that compromised the personal information of 143 million individuals. Drawing on signalling theory, we suggest that such corrective actions like leadership changes or policy reforms signal to the market that the firm is addressing the issue and committed to improving its resilience. These signals can help restore investor confidence and rebuild trust. Therefore, we argue that firms facing their first cyber-attack are likely to experience a more negative stock price reaction than during subsequent incidents.

Overall, those above arguments lead to the following hypothesis.

H_2: Negative short-term reaction to the cyber-attacks to be pronounced when (a) incident appears in the widely known news media, (b) incidents are more severe and (c) incidents occur for the first-time.

The stock market reaction to a cyber-attack may not be uniform across firms due to cross-sectional variation. Specifically, market participants tend to hold a favourable perception of firms with a strong reputation for data security. However, when such firms are breached, the negative impact is often more pronounced. For instance, Equifax, Target, and Sony were perceived to have robust security systems, yet experienced significant stock price declines after cyber-attacks.[11] This may stem from a sense of betrayal and loss of trust among investors, which amplifies the market reaction. Based on signalling theory, we argue that a breach in a highly secure firm may contradict prior signals of reliability and competence, thus sending a negative signal to the market. The breach is likely to generate more negative word-of-mouth, further harming the firm's reputation and performance. This aligns with Labrecque et al. (2021), who show that social stress and social contract theory influence data breach outcomes. Moreover, firms perceived to be secure often attract broader media coverage when breached, increasing the perceived severity of the attack. This can intensify concerns about operational failure and disruption, contributing to sharper declines in stock value.

Investors' reaction to cyber-attack news is also influenced by the nature of the business and sector-specific risk exposure. Cyber-attacks may not affect all sectors equally; certain sectors are more frequently targeted than others. Empirical studies indicate that cyber-attack distribution varies across sectors, with the financial sector being one of the most vulnerable (Aldasoro et al., 2022; Tosun, 2021). Furthermore, while cyber-attacks can cause significant operational disruptions, their financial repercussions differ across sectors. Sectors such as financial services, energy, and retail are among the primary targets of hackers, digital espionage, and other cyber threats.[12] The cyber-attack in the financial sector has immediate and wider effect on the customer data and financial loss, and systemic operational vulnerability. The affected firm is going to experience a severe regulatory penalty and a loss of customer confidence. The attack on the energy sector has the potential to disrupt the economy

[11] See https://www.tripwire.com/state-of-security/relation-between-breaches-and-stock-price-drops.

https://www.bbc.co.uk/news/business-13343205.

[12] The statistics of cyber-attack across the sectors are described in the World Economic Forum in the title "These sectors are top targets for cybercrime, and other cybersecurity news to know this month". Visit here to have comprehensive view: https://www.weforum.org/agenda/2024/04/cybercrime-target-sectors-cybersecurity-news/.

through supply chain interruptions, increased inflation, and threats to national security. Similarly, a cyber-attack on a firm in the retail sector can cause the loss of personal and financial information of customers, leading to identity theft, financial fraud, and a loss of customer trust. Since they heavily rely on digital infrastructure and sensitive data, firms in these three sectors face heightened financial and reputational risks following a cybersecurity breach. According to Cost of a Data Breach Report of 2023 by IBM security, the average cost of data breach in financial, energy and retail sectors are $5.9 million, $4.75 million and $2.96 million, respectively. Moreover, the high financial risk of these sectors is also highlighted in other reports like ENISA Threat Landscape 2024,[13] Sophos 2024 Threat Report[14] and Retail Sector Threat Intelligence Report.[15] Given monetary effect, the nature of sensitive information, complex and integrated operational set up, we expect that any cyber-attack on the firm within the financials, energy and retail sector are likely to face more negative market reaction. Overall, the above arguments lead to construct the following hypothesis,

H_3: Negative stock price effect will be larger for (a) firms with stronger data security prior to incident and (b) firms from vulnerable sectors in terms of cost of data breach i.e., financials, energy and retail sector.

2.1 Conceptual Framework

Figure 1 illustrates the conceptual framework of our study. Firstly, we expect that investors react negatively to the cyber-attacks news (H1). However, our main contribution is to analyse the variation in stock price reaction according to news source influence, severity of the cyber-attacks and novelty (newness) of the event. So, we aim to categorize the news source by low and high influential media, incident severity by its consequential effect and novelty by first-time or repetition of the cyber-attacks for the affected firms. We then predict the stock price reaction based on this heterogeneity (H2). Finally, we predict cross-sectional effect of data privacy policy and business sector on investor reactions (H3).

3 Research Method

3.1 Data and Sample

We cover US-listed firms that experienced cyber-attacks from 2012 to 2022.[16] Numerous country-specific data shows that the US is among the nations experiencing the highest number of cyber incidents. Every three in four companies face the risk of cyber-attack, making cybercrime one of the primary threats for businesses in the US. Furthermore, the estimated loss for the US business sector is more than $ 452 billion due to cybercrime.[17] Moreover, US provides an ideal setting for the study due to more mature stock market and more media coverage.

We use data on news articles concerning cyber-attacks from RepRisk. The advantage of RepRisk is that it combines artificial intelligence and machine learning with highly trained analysts to track corporate incident and quantify their risk from over 150,000 public news sources on daily basis. Its dataset covers 310,000 companies (6% are listed) globally that are associated with risk incidents.[18] After standard filtering of data, excluding stock returns needed for

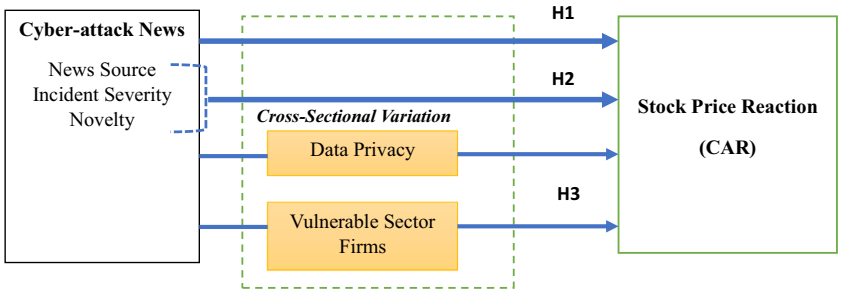

Fig. 1 Conceptual framework. This figure shows the conceptual framework of this study. Appendix 1 provides detailed definitions of the variables

[13] See it here: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[14] See it here: https://www.sophos.com/en-us/content/security-threat-report.

[15] See it here: https://www.quorumcyber.com/wp-content/uploads/2023/08/Quorum-Cyber_Retail-Sector-Threat-Profile-Report.pdf.

[16] While RepRisk began collecting data on various types of corporate incidents as early as 2007, its coverage of cyber-attack-specific events is more limited in the initial years. The first recorded cyber-attack event in RepRisk appears in 2011 in our dataset; however, the number of incidents documented that year is sparse and lacks the statistical significance necessary for meaningful event study analysis. Starting our sample in 2012, when cyber-attack reporting in RepRisk becomes more consistent and frequent, allows us to capture a sufficiently large and reliable dataset necessary to draw robust conclusions about stock market responses.

[17] See the report here: https://www.statista.com/topics/1731/smb-and-cyber-crime/#editorsPicks.

[18] See here https://www.reprisk.com/news-research/resources/methodology.

event studies and confounding financial news, we ended up with a total of 776 news articles about cyber-attacks related to US listed firms.

For stock return data, we use CRSP. For variables in the cross-sectional study, we obtain data from the Compustat and the LSEG (Formerly known as Refinitiv Eikon). We performed pooled OLS regression analysis in our cross-sectional study.

3.2 Event Study Methodology

To capture the stock price reaction to cyber-attacks news, we use event study method. Event study methodology is a statistical technique used to assess the impact of a specific event on the stock price of a company. By analysing stock returns around the time of the event, researchers can isolate the event's effect from other market movements. This method involves calculating the expected normal return during the estimation window and then comparing it to the actual return on the event day. The difference, known as the abnormal return, indicates the impact of the event on the stock price. Event study mitigates reverse causality problem as it captures immediate market reaction. Event study is also popular in information systems research (Konchitchki & O'Leary, 2011). The event study methodology is particularly appropriate for examining short-term stock price reactions to cyber-attacks news for several reasons. First, cyber-attacks are sudden and discrete events, making it easier to pinpoint an exact event date for analysis. Second, the financial market's reaction to such news is typically swift, allowing researchers to capture immediate changes in stock prices. Third, cyber-attacks can have significant implications for a firm's operations, and financial performance, which are quickly reflected in stock prices.

For our event study, we use Fama–French three factor model (Fama & French, 1996) to estimate expected returns, with an estimation window of 250 trading days ending 50 days before the event date (t=0), ensuring no overlap with the event period. Our event study methodology is carried out in the following steps:

1) Abnormal Return (AR): AR for firm *i* on day *t* (AR_{it}) is calculated as the difference between the actual return (R_{it}) and the expected return ($E[R_{it}]$) from the Fama–French model:

$$AR_{it} = R_{it} - E\left[R_{it}\right] \tag{1}$$

where

$$E\left[R_{it}\right] = \alpha_i + \beta_{i1}\left(R_{mt} - R_{ft}\right) + \beta_{i2}SMB_t + \beta_{i3}HML_t \tag{2}$$

R_{mt} is the contemporaneous market return, R_{ft} is risk free rate, α_i is a constant term for firm i and β_i is the slope of the characteristic return of firm i, with the parameters of the model (α_i and β_i) estimated over a period prior to the event. Size factor SMB ('small minus big') is the difference in return between portfolio of small and large firms, and value factor HML ('high minus low') is the difference in return between portfolio of firms with a high book-to-market ratio and a portfolio of firms with a low book-to-market ratio.

2) Average Abnormal Return (AAR): AAR on day *t* aggregates AR across all *N* firms:

$$AAR_t = \frac{1}{N}\sum\nolimits_{i=1}^{N} AR_{it} \tag{3}$$

This measures the average market reaction on a given day relative to the event.

3) Cumulative Abnormal Return (CAR): CAR aggregates AAR over a specified event window (e.g., from t1 to t2):

$$CAR\left(t_1, t_2\right) = \sum\nolimits_{t=t_1}^{t_2} AAR_t \tag{4}$$

For instance, CAR [−1, 1] sums AAR from $t=-1$ to $t=1$, reflecting the cumulative impact over three days.

4 Results

4.1 Descriptive Statistics

We start with Fig. 2 which shows historical trend of news on cyber-attacks for the sample firms over the period 2012 to 2022. There was an increasing trend in news reporting of cyber-attacks until 2018, when it reached its peak, after which it started to decline. Several plausible factors contribute to the surge in cyber-attacks in 2018. This year saw a significant rise in ransomware incidents and business email compromise (BEC)[19] attacks, which became increasingly sophisticated and widespread. Additionally, other key drivers behind the heightened cyber threats included state-sponsored hacking, supply chain vulnerabilities, and evolving attack strategies, all of which collectively furled the increase in cyber-attacks during this period. Whereas Table 1 shows results of summary statistics used in cross-sectional analysis. The mean CAR [- 1, 1] is −0.30% around the event day, suggesting that investors react negatively to cyber-attacks news. The mean value of data privacy is 0.50, indicating that half of the sample firms have better data privacy and

[19] See the report here to explore the rise of cyber-attack in 2018: https://www.industryweek.com/technology-and-iiot/article/22026828/cyberattacks-skyrocketed-in-2018-are-you-ready-for-2019.

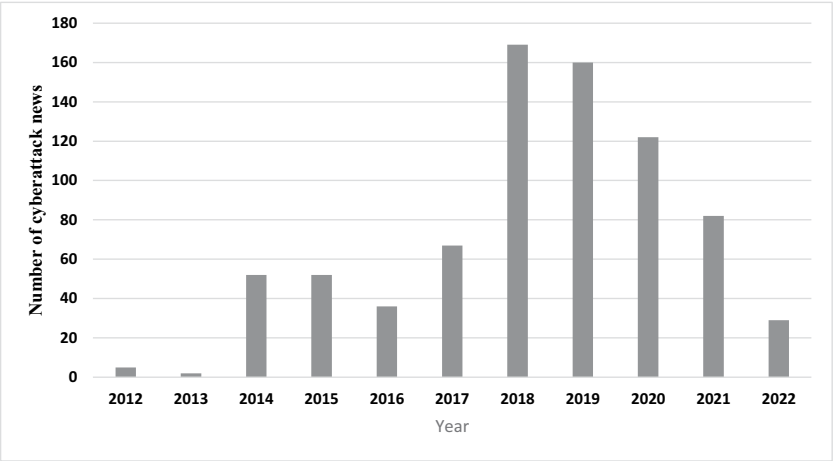

Fig. 2 Trend of cyber-attack news. This figure plots the number of news reporting cyber-attacks from 2012 to 2022 for the sample US listed firms

Table 1 Summary statistics

Variable	Mean	Std. Dev	Min	Max	Obs
CAR % (−1, 1)	−0.303	3.801	−27.84	32.81	776
Data Privacy	0.500	0.500	0	1	748
Vulnerable Sector	0.263	0.4401	0	1	760
Profitability	0.059	0.085	−0.285	0.692	760
Book-to-Market	0.256	0.495	−6.491	3.472	715
Market Capitalisation	206.22	373.68	0.12	2324.4	715
Leverage	0.342	0.216	0	2.802	737
Liquidity	0.165	0.154	0.004	0.790	760
Research & Development	0.047	0.055	0	0.190	446
Capital Expenditure	0.042	0.035	0	0.169	760

The table shows summary statistics of the key variables used in the cross-sectional regression analysis. Appendix 1 provides detailed definitions of the variables

Table 2 Cumulative abnormal return of cyber-attack news

Event Window	CAR (%)	*t*-value
[−1, 0]	−0.28***	−2.71
[0, 0]	−0.15**	−2.16
[0, 1]	−0.18*	−1.65
[−1, 1]	−0.30**	−2.22
[−2, 2]	−0.36*	−1.86
[−5, 5]	−0.39	−1.52
[−10, 10]	−0.19	−0.57
N	776	

This table shows cumulative abnormal return (CAR) of US listed firms around cyber-attack news from 2012 to 2022. We estimate abnormal return using the Fama–French three-factor model. The estimation period is 250 trading days ending 50 trading days before the event date. ***, **, * indicate statistical significance at the 1%, 5% and 10% levels, respectively

security policy. About 26% of sample firms belong to sectors that are largely financially vulnerable due to cyber-attacks. The mean market capitalization is $206 billion, which suggests that target firm are relatively large in size.

4.2 Event Study Results of Cumulative Abnormal Return (CAR)

Table 2 shows the cumulative abnormal returns (CARs) over the different event windows around the day of the cyber-attack news. On the event day, the mean CAR [0, 0] is −0.15% (*t*- value = −2.16). Over a 3-day event window the mean CAR [−1, 1] is −0.30% (*t*-value = −2.22). This supports our H1 that stock market reacts negatively to cyber-attacks news. Economically, the result is also significant. The corresponding average market value loss on the event day is $ 309.33 million (=$ 206217.5 million of average market capitalisation X −0.0015 cumulative abnormal return). This ranges up to $ 618.65 million (=$ 206217.5 million of average market capitalisation X −0.0030 cumulative abnormal return) of market value loss across 3-day event windows [−1, 1]. The mean CAR for the 5-day event window [−2, 2] is −0.36%, with a *t*-value indicating reduced statistical significance compared to the event day [0, 0] and the 3-day event window [−1, 1] CAR. This Suggests that while there is a noticeable negative stock price reaction extending slightly beyond the immediate event period, the effect diminishes in terms of statistical significance as the window widens to five days. For the 11-day event window [−5, 5], the mean CAR remains negative but lacks statistical significance, consistent with the broader event window

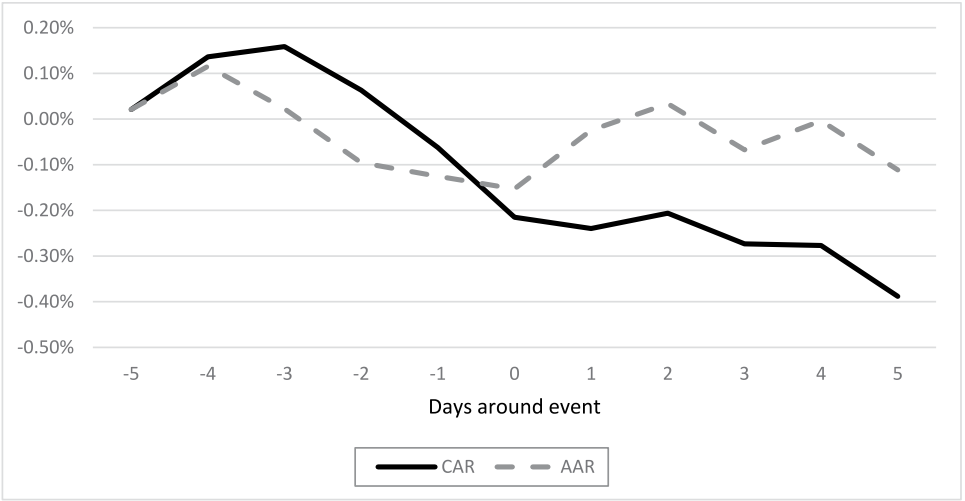

Fig. 3 Cumulative abnormal returns around cyber-attack news. This figure shows daily cumulative average abnormal returns (CARs) around news of cyber-attack (Event Day = 0). We estimate abnormal return using the Fama–French three-factor model. Estimation period is 250 trading days ending 50 trading days before the event date

[−10, 10]. These findings align with the notion of market efficiency, where the impact of cyber-attack news is quickly incorporated into stock prices, primarily within a narrow window around the event day.

Figure 3 shows the daily cumulative and average abnormal returns over a 11-day event window around the publication of cyber-attacks events. This figure clearly demonstrates the significant declines in stock price on the event day for firms that were targets of cyber-attacks.

4.3 Heterogeneity in Cumulative Abnormal Return (CAR)

Table 3 shows the heterogeneity in CAR with respect to news source influence (reach), severity, and novelty (newness) of the event.

Our first heterogeneity analysis is to explore whether the variation in CAR depends on the reach of the news source. Influential news media outlets like CNN and Wall Street Journal (WSJ) are likely to have a greater impact on stock prices than smaller or local news sources because of their broad reach, credibility, and influence. These major outlets have a large audience, including investors and market participants who rely on their coverage for timely and accurate information. When Such prominent media organizations report on significant firm event or corporate news, it tends to gain widespread attention, potentially causing significant shifts in investor sentiment and leading to more pronounced reactions in the stock market. In contrast, local news sources may not have the same high level of credibility or readership, resulting in a more limited impact on stock prices. In our study, we use the RepRisk classification for reach of the

Table 3 Heterogeneity in CAR

Panel A. Reach of News Source				
	Higher-Reach		***Low-Reach***	
Event Window	**CAR (%)**	***t*-value**	**CAR (%)**	***t*-value**
[−1, 0]	−0.29**	−2.36	−0.25	−1.33
[0, 0]	−0.15*	−1.80	−0.16	−1.20
[−1, 1]	−0.41***	−2.58	−0.05	−0.19
N	547		229	
Panel B. Severity				
	Higher-Severity		***Low-Severity***	
Event Window	**CAR (%)**	***t*-value**	**CAR (%)**	***t*-value**
[−1, 0]	−0.33	−1.13	−0.28***	−2.64
[0, 0]	−0.50***	−1.75	−0.14**	−2.01
[−1, 1]	−0.23	−0.53	−0.30**	−2.19
N	18		758	
Panel C. Novelty				
	First-Time		***Reoccurring***	
Event Window	**CAR (%)**	***t*-value**	**CAR (%)**	***t*-value**
[−1, 0]	−0.50*	−1.90	−0.21*	−1.94
[0, 0]	−0.25	−1.34	−0.12*	−1.70
[−1, 1]	−0.79**	−2.42	−0.14	−0.98
N	192		584	

This table shows cumulative abnormal return (CAR) of US listed firms around cyber-attack news from 2012 to 2022 by news source, severity and novelty. Panel A shows results by news source influence, Panel B by severity and, Panel C by novelty of incident. Reach means news source influence. It ranges from low (1) to high (3). We define higher reach when reach level is above 1 i.e., 2 and 3 (e.g., national media or the BBC). Severity means consequence of incidents and ranges from low (1) to high (3). We define higher-severity when severity level is above 1 i.e., 2 and 3. Novelty indicates newness of the incident to the firm, which is for the first-time or re-occurring (repeat). We estimate abnormal return using the Fama–French three-factor model. The estimation period is 250 trading days ending 50 trading days before the event date. ***, **, * indicate statistical significance at the 1%, 5% and 10% levels, respectively

news source. RepRisk classifies news sources by its influence, which ranges from 1 (low) to 3 (high). While RepRisk does not provide raw news sources, its methodology shows what counts as the level of influence of a news source. For example, limited or low-reach sources would include local media, while higher-reach sources include mostly national and regional media, as well as a few global outlets like CNN, The New York Times, or the BBC. In our study, we define higher reach when reach level is above 1 i.e., 2 and 3. Panel A of Table 3 shows the result of CAR by reach of the news source. The mean CAR is up to −0.41% (t-value = −2.58) over [−1, 1] event window. This is consistent with our H2a that negative short-term reaction to the cyber-attack to be pronounced when incident appears in the widely known news media.

Next, we attempt to explore the stock price effect based on the severity of the cyber-attack incident. All cyber-attacks may not have equal consequential effect. For example, a cyber-attack may cause a temporary malfunction in business operations. The ransomware attack on ION Trading Technologies on January 31, 2023, forced its customers to switch to manual trading process. On the other hand, some cyber-attacks may have more consequential effects, Such as the theft of confidential and financial information and Subsequent legal claims. In May 2024, Ticketmaster, one of the world's largest ticket sales and distribution companies, encountered a cyber-attack in which hackers stole the details of 560 million customers. The hackers demanded ransom payment of around £400,000 to stop the data from being sold. RepRisk also classifies event by the severity, which ranges from 1 (low) to 3 (high). We then define higher severity when severity level is above 1 i.e., 2 and 3. Panel B of Table 3 shows the result of CAR by severity of the cyber-attack. On the event day, the mean CAR is −0.50% (t-value = −1.75) for cyber-attacks of higher severity, compared to −0.14% (t-value = −2.01) for low-severity attacks. This supports our H2b that negative short-term reaction to the cyber-attack to be pronounced when incident has more consequential effect.

Our last heterogenous analysis is based on the novelty of the incident, i.e., whether the cyber-attack is the first-time for the firm or a recurring event. When a firm experiences a cyber-attack for the first time, the market perceives it as a significant shock. This initial shock often results in heightened uncertainty and a re-evaluation of the firm's risk profile; thus, investors may react more negatively. On the contrary, when a firm experience repeated cyber-attacks, the market has likely already priced in the associated risks, leading to a less significant reaction, as the news is perceived as less surprising and impactful. Panel C in Table 3 shows the results for CAR based on novelty. We find a more pronounced negative stock price reaction to cyber-attack incidents that occur for the first time compared to repeated ones, which supports our H2c.

4.4 Sub-Sample Period Analysis

In our study, we further explore CAR in two sub-sample periods following the Office of Personnel Management (OPM) data breach and COVID-19. OPM data breach, which occurred in 2015, is considered one of the most significant cyber-attacks in the US history due to the scale and sensitivity of the data compromised. This breach highlighted the risk of data and identity theft, making it a landmark event in the realm of cybersecurity. The event underscored the growing importance of cybersecurity awareness and lead to increased demand for stronger security measures. Table 4 shows the results between two Sub-sample period. Following the announcement of data breach by OPM on June 4 in 2015, our pre-event data breach period is 2012 to June 3, 2015, and post-event data breach period is June 4, 2015 to 2022. We find more negative stock price reaction after OPM data breach period. The OPM breach gave insight about the vulnerability of organizations to cyber-attacks, leading to increased scrutiny on companies' cybersecurity measures. Post-breach, investors became more sensitive to potential costs, causing them to react more strongly to any news related to data security incidents. As a result, companies experienced cyber-attacks after OPM data breach are perceived as having inadequate cybersecurity measurement and therefore, suffered by more negative stock price reaction.

Another sub-sample period analysis is COVID-19. The pandemic has not only brought about accelerated digitalisation and security measures but also reshaped market dynamics and investor sentiment during the crisis period. Therefore, it is important to see how investors

Table 4 CAR of cyber-attack news before and after office of personnel management data breach

	Before OPM data breach (2012-June 3, 2015)		*After OPM data breach (June 4,2015–2022)*	
Event Window	CAR (%)	t-value	CAR (%)	t-value
[−1, 0]	−0.12	−0.80	−0.30***	−2.62
[0, 0]	−0.08	−0.70	−0.16**	−2.07
[−1, 1]	−0.01	−0.58	−0.33**	−2.16
N	81		695	

This table shows cumulative abnormal return (CAR) of US listed firms before and after Office of Personnel Management (OPM) data breach. We estimate abnormal return using the Fama–French three-factor model. The estimated period is 250 trading days ending 50 trading days before the event date. Left panel shows stock price reactions before OPM data breach period and right panel shows stock price reactions after OPM data breach period. ***, ** indicate statistical significance at the 1%, and 5% levels, respectively

perceive cyber-attack risk before and after the pandemic. Our results in Table 5 shows that more negative and significant stock price reaction before COVID-19 period. This is not surprising, as cybersecurity expenditure and measurement have significantly increased since the arrival of COVID-19,[20] reducing investor concern and surprise about the impact.

4.5 Cross-Sectional Analysis

4.5.1 Data Privacy and Stock Price Reaction

In our first cross-sectional analysis, we explore the impact of the data privacy policy on stock price reaction. To test our hypothesis (H3a), we estimate following regression model:

$$\text{CAR [-1, 1]} = \alpha + \beta_1 Data\ Privacy + \gamma\ Controls + Industry\ FE + Year\&Month\ FE + \varepsilon \quad (5)$$

where the dependent variable CAR is the cumulative abnormal returns on the event windows [−1, 1]. The independent variable is Data Privacy, which indicates the policy performance for data privacy and security. The control variables are profitability, book-to-market, firm size, leverage, liquidity, research & development, and capital expenditure, which can affect stock returns. We also capture industry, year and month fixed effects (FE). Appendix 1 provides details of all the variables.

Table 6 presents the empirical results. We find the coefficient estimate for Data Privacy is statistically significant at the 5% level. These results suggest that investors respond more negatively to cyber-attack news for the firms with strong data privacy policies, consistent with H3a.

Firms with strong data privacy policies are generally perceived as being more secure and trustworthy, leading investors to assume that their data is well-protected. When these firms experience a breach, the violation of data protection trust can lead to a stronger negative reaction, as the market perceives the failure as a betrayal of the company's commitment to security and privacy. On the other hand, firms with weaker data privacy policies may not suffer severely in stock price decline in the event of a cyber-attack, as the market may have already priced in the risks associated with inadequate data protection. Investors in these firms might have lower expectations regarding cybersecurity, leading to a less reaction when an attack occurs.

[20] Statista (2024): Spending on cybersecurity worldwide from 2017 to 2024 https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending.

Table 5 CAR of cyber-attack news before and after COVID-19

	Before COVID-19 (2012–2019)		*Post COVID-19 (2020–2022)*	
Event Window	CAR (%)	*t*-value	CAR (%)	*t*-value
[−1, 0]	−0.26***	−2.77	−0.31	−1.20
[0, 0]	−0.15**	−2.32	−0.15	−0.86
[−1, 1]	−0.32***	−2.58	−0.26	−0.74
N	543		233	

This table shows cumulative abnormal return (CAR) of US listed firms before and after COVID-19 period. We estimate abnormal return using the Fama–French three-factor model. The estimated period is 250 trading days ending 50 trading days before the event date. Left panel shows stock price reactions before COVID-19 period (2012–2019) and right panel shows stock price reactions after COVID-19 period (2020–2022). ***, ** indicate statistical significance at the 1%, and 5% levels, respectively

Table 6 The effect of data privacy policy

	(1)	(2)
Variables	CAR [−1, 1]	
Data Privacy	−1.45**	−1.50**
	(−2.123)	(−2.367)
Profitability	−10.7**	−9.43*
	(−2.380)	(−1.754)
Book-to-Market	−0.91***	−0.91***
	(−3.772)	(−3.302)
Firm Size	0.49**	0.45**
	(2.563)	(2.218)
Leverage	1.18	0.614
	(1.135)	(0.514)
Liquidity	1.66	2.25
	(0.903)	(1.238)
Research & Development	−18.7	−13.5
	(−1.403)	(−1.098)
Capital Expenditure	14.2	15.3
	(1.212)	(1.383)
Industry FE	YES	YES
Year FE	YES	NO
YearXMonth FE	NO	YES
N	435	435
R-squared	0.207	0.424

This table shows cross-sectional regressions estimated for the impact of data privacy policy on CARs following news of cyber-attack. The dependent variable is cumulative abnormal return estimated using Fama–French three-factor model. Data Privacy, the indicator variable, is set to 1 if policy data privacy score is above median, and 0 otherwise. Policy data privacy score, obtained from Refinitiv Eikon, measures the process or initiative by which company strives to protect customer and general public privacy including safeguarding or securing confidential data. Appendix 1 provides detailed definitions of the variables. Coefficients are in percentages. The *t*-statistics are in parentheses based on robust standard errors, clustered at the firm level. ***, **, * indicate statistical significance at the 1%, 5% and 10% levels, respectively

4.5.2 Financially Vulnerable Sector and Stock Price Reaction

In our study, we also examine whether stock price reaction to cyber-attacks news depends on the nature of the business of the affected firm. To test our hypothesis (H3b), we estimate following regression model:

$$\text{CAR } [\text{-}1,\ 1] = \alpha + \beta_1 Vulnerable\ Sector + \gamma\ Controls + Year\&Month\ FE + \varepsilon \quad (6)$$

where the dependent variable CAR is the cumulative abnormal returns on the event windows [−1,1]. Vulnerable sector is a dummy variable, indicating whether the business of the firm is under sector of financials, retail and energy, which are more financially vulnerable to cyber-attacks. All other variables are as in Eq. 5.

Table 7 shows the empirical results. The coefficient of vulnerable sector is negative and statistically significant at the 5% level. This supports H3b, that firms under financially vulnerable sector are more negatively affected by the cyber-attacks news. In the financial and retail sector, cyber-attacks can compromise sensitive financial and customer payment related data. In the energy sector, cyber-attacks can disrupt essential services, posing significant operational risks that can be costly to mitigate. Therefore, the potential financial liabilities are often seen as higher in these industries, leading to more pronounced negative reactions in stock prices when such firms are targeted by cyber-attacks.

Table 7 The effect of vulnerable sector

	(1)	(2)
Variables	CAR [−1, 1]	
Vulnerable Sector	−0.84**	−0.94**
	(−2.318)	(−1.996)
Profitability	−10.4*	−10.8
	(−1.911)	(−1.613)
Book-to-Market	−0.81***	−0.78***
	(−4.129)	(−3.804)
Firm Size	0.37*	0.42**
	(1.956)	(1.986)
Leverage	1.79	1.90
	(1.612)	(1.438)
Liquidity	3.09**	3.93**
	(2.023)	(2.240)
Research & Development	−12.1*	−13.6*
	(−1.819)	(−1.870)
Capital Expenditure	20.7**	20.8**
	(2.512)	(2.186)
Industry FE	NO	NO
Year FE	YES	NO
YearXMonth FE	NO	YES
N	441	441
R-squared	0.101	0.295

This table shows cross-sectional regressions estimated for the vulnerable sector impact on CARs following news of cyber-attack. The dependent variable is cumulative abnormal return estimated using Fama–French three-factor model. Vulnerable sector, the indicator variable, is set to 1 if sample firm is under sector which is more financially vulnerable to cyber-attack (financials, energy and retail), and 0 otherwise. Appendix 1 provides detailed definitions of the variables. Coefficients are in percentages. The t-statistics are in parentheses based on robust standard errors, clustered at the firm level. ***, **, * indicate statistical significance at the 1%, 5% and 10% levels, respectively

4.6 Additional Test and Robustness Analysis

Although we report stock price reactions based on the reach of the news source and the severity of the attack, the effect may not be consistent across firms of different sizes. To address this, we categorize our firms into large and small groups using the sample median value of total assets. We present the results of stock price reactions to cyber-attacks with higher reach and severity, comparing small and large firms, in Table 8. We find that small firms are more negatively affected by media influence and attack severity. Small firms may be more vulnerable due to limited resources for cybersecurity and recovery, amplifying investor concerns about operational and reputational damage. Their lower visibility and market resilience likely heighten sensitivity to credible media exposure, as investors perceive greater risk. Conversely, large firms, with diversified operations and stronger risk management, may effectively mitigate such shocks.

We also reexamine stock price reaction and cross-sectional analysis using alternative event study method. We use Carhart four factor model (Carhart, 1997). The Carhart four-factor model is an alternative to the Fama–French three-factor model in examining stock price reactions to cyber-attack news because it adds a momentum factor to the existing

Table 8 Stock price reaction by firm size

	(1)	(2)	(3)	(4)
	Small Firms		Large Firms	
Event Window	*Higher -Reach*	*Higher -Severity*	*Higher-Reach*	*Higher-Severity*
[−1, 1]	−0.79***	−1.21*	−0.06	0.15
	(−2.72)	(−2.15)	(−0.42)	(0.27)
N	261	5	286	13

This table shows firm size variation in cumulative abnormal return (CAR) of US listed firms around cyber-attack news from 2012 to 2022 by news source and severity. We estimate abnormal return using the Fama–French three-factor model. The estimation period is 250 trading days ending 50 trading days before the event date. Reach means news source influence. It ranges from low (1) to high (3). We define higher reach when reach level is above 1 i.e., 2 and 3. Severity means consequence of incidents and ranges from low (1) to high (3). We define higher-severity when severity level is above 1 i.e., 2 and 3. Firm size is based on median value of total assets. ***, * indicate statistical significance at the 1% and 10% levels, respectively

three factors (market risk, size, and value). The momentum factor captures the tendency of stocks that have performed well or poorly in the past to continue to do so in the future. This is particularly relevant in the context of cyber-attacks, as market sentiment and investor behaviour can be significantly influenced by recent stock performance, making the Carhart model more comprehensive for such event studies. Table 9 shows event study results. Column (1) shows results of full sample, Column (2) includes of higher-reach news source only, Column (3) includes incidents of higher-severity only, and Column (4) includes cyber-attacks for the first time. The results remain robust and similar to previous findings. For our cross-sectional analysis, we also use CAR as dependent variable estimated based on Carhart four factor model. Table 10 shows the results. Our results remain consistent to the original findings.

5 Discussion

Our study highlights the growing concern over cybersecurity threats and the increasing frequency of cyber-attacks, reinforcing the financial materiality of cybersecurity risk. The significant negative stock market reaction to cyber-attack news underscores the tangible financial consequences associated with such incidents. However, the extent of market impact is not homogeneous; rather, it is shaped by several key factors, including media influence, severity, and novelty. The role of media in shaping market sentiment cannot be overstated. High-reach news sources amplify investor concerns, leading to more pronounced stock price declines. Similarly, severity plays a crucial role, as cyber-attacks that cause significant operational disruptions or data breaches trigger stronger market reactions than those with minimal consequences. Novelty also influences investor behaviour. First-time cyber-attacks tend to cause greater market volatility as they introduce new uncertainty, whereas repeated incidents may lead to more measured responses as investors adjust their risk expectations over time.

Furthermore, external events such as the post-OPM data breach and post-COVID-19 era have reshaped investor

Table 9 Stock price reaction using alternate event study method (as Robustness)

	(1)	(2)	(3)	(4)
	CAR (%)			
Event Window	*Full Sample*	*Higher-Reach*	*Higher-Severity*	*First-Time*
[−1, 0]	−0.26**	−0.28**	−0.31	−0.44*
	(−2.50)	(−2.25)	(−1.09)	(−1.65)
[0, 0]	−0.14*	−0.13	−0.49*	−0.19
	(−1.90)	(1.58)	(−1.93)	(−0.99)
[−1, 1]	−0.27***	−0.40**	−0.22	−0.70**
	(−2.00)	(−2.51)	(−0.52)	(−2.06)
N	776	548	18	198

This table shows cumulative abnormal return (CAR) of US listed firms around cyber-attack news from 2012 to 2022. We estimate abnormal return using the Carhart four-factor model as alternated event study. The estimation period is 250 trading days ending 50 trading days before the event date. Column (1) shows results for full sample, Column (2) shows results by news source influence, Column (3) shows results by severity and Column (4) shows results by novelty of incident. Reach means news source influence. It ranges from low (1) to high (3). We define higher reach when reach level is above 1 i.e., 2 and 3. Severity means consequence of incidents and ranges from low (1) to high (3). We define higher-severity when severity level is above 1 i.e., 2 and 3. Novelty indicates newness of the incident to the firm, which is for the first time or re-occurring (repeat). ***, **, * indicate statistical significance at the 1%, 5% and 10% levels, respectively

Table 10 Cross-Sectional Effect of CAR using Alternate Event Study Model (as Robustness)

	(1)	(2)	(3)	(4)
Variables	CAR [−1, 1]			
Data Privacy	−1.43**	−1.46**		
	(−2.106)	(−2.416)		
Vulnerable Sector			−0.96***	−01.12**
			(−2.677)	(−2.487)
Profitability	−1.14***	−9.88*	−10.9**	−11.2*
	(−2.639)	(−1.973)	(−2.076)	(−1.749)
Book-to-Market	−0.87***	−0.89***	−0.83***	−0.80***
	(−3.751)	(−3.656)	(−4.398)	(−3.886)
Firm Size	0.44**	0.39**	0.28	0.34
	(2.353)	(2.038)	(1.471)	(1.584)
Leverage	1.39	0.64	1.80*	1.74
	(1.367)	(0.566)	(1.662)	(1.362)
Liquidity	2.15	2.93*	3.16**	4.00**
	(1.157)	(1.675)	(2.090)	(2.388)
Research & Development	−19.4	−14.8	−12.4*	−14.2**
	(−1.479)	(−1.231)	(−1.887)	(−2.030)
Capital Expenditure	18.6	17.9	23.8***	23.2**
	(1.524)	(1.659)	(2.941)	(2.538)
Industry FE	YES	YES	NO	NO
Year FE	YES	NO	YES	NO
YearXMonth FE	NO	YES	NO	YES
N	435	435	441	441
R-squared	0.216	0.443	0.109	0.319

This table shows cross-sectional regressions using alternated event study model. CARs are estimated using Carhart four-factor model. The dependent variable is cumulative abnormal return. Data Privacy, the indicator variable, is set to 1 if policy data privacy score is above median, and 0 otherwise. Policy data privacy score, obtained from Refinitiv Eikon, measures the process or initiative by which company strives to protect customer and general public privacy including safeguarding or securing confidential data. Vulnerable sector, the indicator variable, is set to 1 if sample firm is under sector which is more financially vulnerable to cyber-attack (financials, energy and retail), and 0 otherwise. Appendix 1 provides detailed definitions of the variables. Coefficients are in percentages. The *t*-statistics are in parentheses based on robust standard errors, clustered at the firm level. ***, **, * indicate statistical significance at the 1%, 5% and 10% levels, respectively

perceptions about cybersecurity risks. These events have driven firms to reassess their cybersecurity investments, highlighting the evolving landscape of corporate vulnerability and resilience. As cybersecurity awareness increases, so does investor scrutiny, affecting how the market reacts to breaches. Importantly, regulatory scrutiny, potential penalties, and concerns over reputational damage and litigation costs vary across industries, contributing to differing stock market reactions. Sectors such as finance, retail, and energy are particularly susceptible to heightened negative responses, as cyber-attacks in these industries pose greater financial and operational risks. Finally, an intriguing paradox emerges regarding data privacy policies. Firms with stronger data privacy measures experience more severe stock price declines following a breach, suggesting that market expectations for security are higher for these firms. When such organizations fall victim to cyber-attacks, the perceived breach of trust and security commitment is more damaging, leading to heightened investor concerns and stronger negative market reactions.

6 Conclusion

As businesses increasingly adopt digitalization, a major concern is the rising cyber security risk across all industries. These attacks lead to a decline in investor confidence, negatively impact market sentiment and ultimately affect the stock performance of the targeted companies. This study therefore aims to examine the stock price reaction to the cyber-attack news in general. Specifically, the study explores how the stock price is affected by factors, such as the media coverage of the event, the intensity of the cyber-attack, and firm-specific attributes. To capture the impact derived from cyber-attack event, this study applies event study approach to a relatively novel large dataset from the US economy.

Our study adds several contributions. First, we advance the growing body of research on the value relevance of cybersecurity breaches by employing a large and recent dataset, effectively addressing selection bias concerns that have been prevalent in prior studies. By utilizing a broader and more contemporary sample, our findings offer more generalizable and robust insights into the financial impact of cyber-attacks. For example, our findings show that the stock price of the cyber-attacked firm significantly falls on the event day, signifying the value relevance of cyber-attack news for investors. Second, we provide novel evidence on the role of media influence, incident severity, and event novelty in shaping investor reactions as these aspects were largely unexplored in previous research. We are the first to empirically examine how the credibility and popularity of news platforms reporting a cyber-attack affect investor responses. Our empirical findings provide further insights, such as the short-term negative reaction to a cyber-attack event being more pronounced when the incident is covered by widely recognized news media, highlighting the importance of source credibility. Our results show that the value destruction also depends on the severity of the impact. We also observe a change in investors' risk perception following subsequent cyber-attacks, with the negative effect being more pronounced for firms experiencing a cyber-attack for the first time compared to those experiencing repeated attacks. Third, our study contributes to the understanding of how rising awareness of cyber threats influences investor behaviour. We find that heightened cybersecurity awareness following major breaches, such as the Office of Personnel Management (OPM) data breach, intensifies market reactions. Additionally, our results highlight that the COVID-19 pandemic altered risk perceptions, leading to differing investor responses before and after the pandemic. Finally, our study provides cross-sectional evidence on the valuation of data privacy policies and sector-specific vulnerabilities in the wake of cyber-attack reporting. Cross-sectional analysis shows that investors respond more negatively to cyber-attack news for the firms with strong data privacy policies. This suggests that strong data privacy policies foster greater trust among investors, and violations of such trust due to data privacy breaches lead to a reduction in stock value, primarily because of the sense of betrayal. We also find the stock value destruction effect varies across the nature of the business where cyber-attack affects financial, retail and energy sector more severely than others.

6.1 Theoretical and Practical Implication

This study offers several theoretical and practical implications for academia, industry practitioners, investors, and regulatory bodies. From a theoretical perspective, it advances the understanding of cybersecurity risk in financial markets by extending the application of signalling theory demonstrating that media reputation amplifies the impact of signals, and the signalling effects are dynamic over time and cyber incidents. Additionally, it contributes to the efficient market hypothesis (EMH) literature by examining the speed and intensity with which cyber-attack news is reflected in stock prices. The study also suggests that market reactions to such events change over time as investors revise their beliefs, incorporating behavioural elements such as trust and perceived firm credibility. Our findings suggest that cyber-attacks act as a negative signal to investors, leading to an immediate decline in market value. The differential market reactions based

on media influence, breach severity, and firm-specific characteristics provide empirical support for the semi-strong form of EMH, which posits that stock prices adjust rapidly to publicly available information. Moreover, the overreaction to first-time cyber-attacks suggests that investors may not always process information similarly and rationally, aligning with insights from behavioural finance theories, particularly loss aversion and bounded rationality. Additionally, our research enriches the theoretical discourse on information asymmetry and media effects in financial markets. For example, market reacts intensely when cyber-attacks are reported by high-credibility media platforms that reinforces the notion that media channels influence the perceived severity and credibility of negative corporate events. This aligns with theories on framing effects and selective attention, suggesting that investors rely on media sources to interpret risk and adjust their investment decisions accordingly.

Practically, this study also offers several implications for industry practice, investors and regulatory bodies. First, our findings underscore the critical need for firms to implement robust cybersecurity measures and proactive management strategies to safeguard firms' digital infrastructure system. Second, organizations must adopt a dynamic and wider approach to cybersecurity that includes continuous monitoring, threat intelligence integration, and incident response preparedness. This is because of the increasing frequency, evolving dynamics and sophistication of cyber-attacks. Third, firms should be strategic in their communication about cyber incidents, taking into account the nature of the attack, potential reputational risks, and evolving public sentiment. This is crucial, as carefully managing the disclosure of a cyber-attack can help maintain stakeholder trust while minimizing adverse effects on market perception. Finally, regulatory bodies also need to play a crucial role in shaping a cyber-resilient business environment by establishing and enforcing comprehensive cybersecurity guidelines, policies, and frameworks that help firms navigate the evolving threat landscape effectively. For example, regulatory guidelines on cyber-attack disclosure, the platform to disclosure, the contents to disclose and how fast to disclose and the depth and breadth of disclosures.

Beyond internal security measures, our findings have significant implications for the investment community. For example, investors should consider investment decision wisely when there is a cyber-attacks information is reported. Investors need to consider investment horizons, and industry-specific vulnerabilities, the news media platform where the cyber-attack news appears, and the type and history of cyber-attack. This is because the severity of an attack and the market's response may vary across industries, requiring investors to adopt a nuanced approach in assessing cyber risk exposure. While firms need to demonstrate strong cybersecurity governance and transparent incident management to maintain investor confidence and long-term financial stability, they must also ensure continuous improvement in their security systems. Therefore, both firms and investors must stay alert to shift cybersecurity landscape, leveraging insights from cyber incidents to inform strategic decision-making and risk management practices.

6.2 Limitations and Future Research Direction

There are some limitations of our study. Future research addressing these constraints could build on our findings and offer a more comprehensive view of how cyber-attack news shapes market behavior across diverse contexts. First, our study relies on data from RepRisk, which, while comprehensive with 776 cyber-attack incidents from 2012 to 2022, may not capture all cyber-attacks affecting US listed firms. Some incidents might go unreported or lack sufficient media coverage to be included. Second, our analysis focuses on short-term stock price reactions, which may not fully capture long-term impacts on firm value or investor sentiment. Cyber-attacks could have delayed effects such as prolonged reputational damage that extend beyond our observation period. Third, our focus on US listed firms limits the generalizability of findings to other markets with differing regulatory environments or media landscapes, or cybersecurity awareness. Lastly, while we account for news source influence, severity, and novelty, other factors such as the type of cyber-attack (e.g., ransomware vs. data theft) are not fully explored due to data constraints.

However, cybersecurity risk remains a highly relevant and pressing issue, which requires further research in this area. As cyber threats continue to evolve, there are several critical areas where further research can provide valuable insights. For example, future research can investigate the sentiment and tone of cyber-attack news, as well as the modes of cyber-attack information dissemination. This will help to understand how these factors influence investor reactions. Additionally, future studies can explore the cross-border diffusion of stock price reactions to cyber-attacks, examining whether market responses vary across different countries and regulatory environments. Further research can also analyse how different types of investors such as institutional versus retail investors interpret and respond to cyber-attack news, providing deeper insights into market behaviour and investment decision-making in the face of cybersecurity risks.

Appendix 1. Variable description

Variable	Definition	Data Source
CAR	Cumulative abnormal return.	*CRSP*
Reach	News source influence from RepRisk rating. It ranges from low (1) to high (3). We define higher reach when reach is 2 and 3. Limited or low reach sources would include local media, smaller NGOs, local governmental bodies, and social media. Medium reach sources include most national and regional media, international NGOs, and state, national, and international governmental bodies. High reach sources are the few truly global media outlets like BBC, CNN, Financial Times.	*RepRisk*
Severity	Consequence of incidents from RepRisk rating. It ranges from low (1) to high (3). We define higher severity when severity is 2 and 3.	*RepRisk*
Novelty	Newness of the incident. RepRisk identifies whether it is the first time a com pany/project is exposed to a specific ESG Issue.	*RepRisk*
Data Privacy	The indicator variable is set to 1 if policy data privacy score is above median, and 0 otherwise. Policy data privacy score, obtained from Refinitiv Eikon, measures the process or initiative by which company strives to protect customer and general public privacy including safeguarding or securing confidential data.	*LSEG (Refinitiv Eikon)*
Vulnerable Sector	The indicator variable is set to 1 if sample firm is under sector which is more financially vulnerable to cyber-attacks (financials, energy and retail), and 0 otherwise. Identification of vulnerability sector is based on cost of data breach following 'Cost of a data breach' report-2023 by IBM security.	
Profitability	Net income after tax over total assets.	*Compustat*
Book-to-Market	Book value of equity over market value of equity.	*Compustat*
Firm Size	Natural logarithm of market Capitalisation. In summary statistics, we show this in billion $.	*Compustat*
Leverage	Debt to total Assets.	*Compustat*
Liquidity	Cash and short-term investments over total assets.	*Compustat*
Research & Development	Research and development expenditure over total assets.	*Compustat*
Capital Expenditure	Capital expenditure over total assets.	*Compustat*

Acknowledgements The authors would like to thank Ram Ramesh and H. Raghav Rao, Editors-in-Chief; Seun Kolade, the lead guest editor; along with all the editors of the special issue and the reviewers for their valuable feedback. The authors also wish to thank the participants and discussants at the 14th Counter Fraud, Cybercrime, and Forensic Accounting Conference in Portsmouth for their constructive feedback.

Authors' Contributions Dewan contributed to the study idea formulation, conceptual design, hypothesis formulation, methodology and data analysis. Hakim worked on the literature review and hypothesis writing. Dewan and Hakim both collaborated on discussion, findings and implications. The manuscript was improved by all authors in the final version. Both authors approved the final manuscript.

Funding No funding was received. The authors have no financial or proprietary interests in any material discussed in this article.

Data Availability Available upon reasonable request with the permission of data vendor.

Declarations

Ethics Approval and Consent to Participate Not applicable.

Consent for Publication Authors agreed with the content, and all gave explicit consent to submit. Participants/institutional consent is not applicable.

Competing interests All authors declare that they have no conflicts of interest.

References

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability, 60*, 100989.

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.

Bai, C., Gao, W., & Sarkis, J. (2021). Operational risks and firm market performance: Evidence from China. *Decision Sciences, 52*(4), 920–951.

Barkemeyer, R., Faugère, C., Gergaud, O., & Preuss, L. (2020). Media attention to large-scale corporate scandals: Hype and boredom in the age of social media. *Journal of Business Research, 109*, 385–398.

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.

Cao, H., Phan, H. V., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis, 93*, 103164.

Capelle-Blancard, G., & Laguna, M. A. (2010). How does the stock market respond to chemical disasters? *Journal of Environmental Economics and Management, 59*(2), 192–205.

Carhart, M. M. (1997). On persistence in mutual fund performance. *The Journal of Finance, 52*(1), 57–82.

Carlini, F., Cucinelli, D., Previtali, D., & Soana, M. G. (2020). Don't talk too bad! Stock market reactions to bank corporate governance news. *Journal of Banking & Finance, 121*, 105962.

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.

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

Cready, W. M., & Gurun, U. G. (2010). Aggregate market reaction to earnings announcements. *Journal of Accounting Research, 48*(2), 289–334.

Davidson, W. N., Worrell, D. L., & Lee, C. I. (1994). Stock market reactions to announced corporate illegalities. *Journal of Business Ethics, 13*, 979–987.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119.

Fama, E. F., & French, K. R. (1996). Multifactor explanations of asset pricing anomalies. *The Journal of Finance, 51*(1), 55–84.

Flammer, C. (2013). Corporate social responsibility and shareholder reaction: The environmental awareness of investors. *Academy of Management Journal, 56*(3), 758–781.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies, 36*(1), 351–407.

Foecking, N., Wang, M., & Huynh, T. L. D. (2021). How do investors react to the data breaches news? Empirical evidence from Facebook Inc. during the years 2016–2019. *Technology in Society, 67*, Article 101717.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information and ManagemeNt, 46*(7), 404–410.

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.

Hao, J., & Xiong, X. (2021). Retail investor attention and firms' idiosyncratic risk: Evidence from China. *International Review of Financial Analysis, 74*, 101675.

Hillert, A., Jacobs, H., & Müller, S. (2014). Media makes momentum. *The Review of Financial Studies, 27*(12), 3467–3501.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches? *The Accounting Review, 96*(3), 261–286.

Jamilov, R., Rey, H., & Tahoun, A. (2023). *The anatomy of cyber risk (No. w28906)*. National Bureau of Economic Research.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681–695.

Jiang, H., Khanna, N., Yang, Q., & Zhou, J. (2024). The cyber risk premium. *Management Science, 70*(12), 8791–8817.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749.

Kaplanski, G., & Levy, H. (2010). Sentiment and stock prices: The case of aviation disasters. *Journal of Financial Economics, 95*(2), 174–201.

Kölbel, J. F., Busch, T., & Jancso, L. M. (2017). How media coverage of corporate social irresponsibility increases financial risk. *Strategic Management Journal*, *38*(11), 2266–2284.

Konchitchki, Y., & O'Leary, D. E. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems, 12*(2), 99–115.

Krüger, P. (2015). Corporate goodness and shareholder wealth. *Journal of Financial Economics, 115*(2), 304–329.

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research, 135*, 559–571.

Lansing, K. J. (2019). Real business cycles, animal spirits, and stock market valuation. *International Journal of Economic Theory, 15*(1), 77–94.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review, 53*(2), 413–455.

Martins, A. M., & Moutinho, N. (2025). Stock-term market impact of major cyber-attacks: Evidence for the ten most exposed insurance firms to cyber risk. *Finance Research Letters, 71*, 106361.

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance-Issues and Practice, 45*, 580–615.

Nordlund, J. (2019). *The* role *of experience in the director labor market: Evidence from cybersecurity events*. Louisiana State University Unpublished working paper.

Pevzner, M., Xie, F., & Xin, X. (2015). When firms talk, do investors listen? The role of trust in stock market reactions to corporate earnings announcements. *Journal of Financial Economics, 117*(1), 190–223.

Pornpitakpan, C. (2004). The persuasiveness of source credibility: A critical review of five decades' evidence. *Journal of Applied Social Psychology, 34*(2), 243–281.

Rhee, E. Y., & Fiss, P. C. (2014). Framing controversial actions: Regulatory focus, source credibility, and stock market reaction to poison pill adoption. *Academy of Management Journal, 57*(6), 1734–1758.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*(1), 74–104.

Shaikh, F. A., & Siponen, M. (2024). Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions. *Information Systems Frontiers, 26*(3), 1109–1120.

Song, C., & Han, S. H. (2017). Stock market reaction to corporate crime: Evidence from South Korea. *Journal of Business Ethics, 143*, 323–351.

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

Su, W., Peng, M. W., Tan, W., & Cheung, Y. L. (2016). The signaling effect of corporate social responsibility in emerging economies. *Journal of Business Ethics, 134*, 479–491.

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems, 98*, 660–671.

Tetlock, P. C. (2007). Giving content to investor sentiment: The role of media in the stock market. *The Journal of Finance, 62*(3), 1139–1168.

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

Tripathi, M., & Mukhopadhyay, A. (2020). Financial loss due to a data privacy breach: An empirical analysis. *Journal of Organizational Computing and Electronic Commerce, 30*(4), 381–400.

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems, 35*(1), 155–186.

Wu, C. H., & Lin, C. J. (2017). The impact of media coverage on investor trading behavior and stock returns. *Pacific-Basin Finance Journal, 43*, 151–172.

Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. *International Review of Financial Analysis, 93*, Article 103174.

Dewan Muktadir-Al-Mukit Dr. Dewan Mukit is a Senior Lecturer in Finance at Sheffield Business School, Sheffield Hallam University. He holds a PhD in Accounting and Finance from the University of Liverpool. Dr. Mukit has published several articles in high-impact, peer-reviewed journals, including the *Journal of International Financial Markets, Institutions and Money* and *Business Strategy and the Environment*. His book chapter on green financing has been published by Routledge. He serves as a reviewer for the *International Review of Financial Analysis* and *Finance Research Letters* journals. His research area focuses on FinTech, stock markets, climate finance, biodiversity finance, corporate governance, and ESG. At Sheffield Business School, he co-leads a research working group on "FinTech and Financial Inclusion".

Md Hakim Ali Dr. Hakim is a Lecturer in Finance at the Department of Finance and Economics at Manchester Metropolitan University. He holds a PhD in Finance and Banking. His project-based doctoral research addresses how cybersecurity hazards increase banking operational risks in a technology-driven financial system and destabilise the global financial sector. His research interests encompass risk management, capital markets, cryptocurrencies, regulatory technology (RegTech), and cyber economics. His research has been published in several academic journals, including *Technological Forecasting and Social Change, International Review of Financial Analysis, International Journal of Finance and Economics, Economic Modelling, Australian Economic Papers, Risk Management, Managerial Finance*, and *Studies in Economics and Finance*, among others.