HACKED:
Understanding the Stock Market Response to Cyberattacks

Erdinc Akyildirim[a,b], Thomas Conlon[c#], Shaen Corbet[d,e*], Yang (Greg) Hou[e]

[a] *School of Management, University of Bradford, Bradford, UK*

[b] *Department of Banking and Finance, University of Zurich, Zurich, Switzerland*

[c] *Smurfit Graduate School of Business, University College Dublin, Ireland*

[d] *DCU Business School, Dublin City University, Dublin 9, Ireland*

[e] *School of Accounting, Finance and Economics, University of Waikato, Hamilton 3240, New Zealand*

[*] *Corresponding author: e. shaen.corbet@dcu.ie; t. +353 1 700 5993*

Abstract

Increasing levels of digitisation makes firms more susceptible to cyberattacks and privacy violations. In this paper, we quantify the impact of cybercrime on company stock returns, using a large international sample. In the day after the cyber event, stock returns are found to decrease by -0.25% but the effect reverses in about two weeks. The magnitude of the stock market decrease is greatest for companies which have experienced reoccurring events and for breaches deemed to be severe. Finally, we show that the extent of the stock market decline is related to company specific characteristics, including size, volatility, credit ranking and asset volatility. The empirical results highlight important policy and regulatory issues, not least the need for cyber risk disclosure requirements.

Keywords: Reputation; Cyber Attack; Privacy Violation; Global Financial Markets; Corporate Resilience; Social Responsibility.

JEL Classifications: G14; G32; G38; O38.

[#]Conlon acknowledges the support of Science Foundation Ireland under Grant Number 16/SPP/3347 and 13/RC/2106 and 17/SP/5447.

1. Introduction

In 2010, computer hackers stole millions of names and email addresses from the marketing email provider Epsilon. Among the most significant hacks in history, this not only impacted the company in question, but also dozens of large companies including JPMorgan, Citigroup, Best Buy and Disney. McKinsey, the global management consulting company, estimate that the economic damage from cyberattacks will reach $10.5 trillion annually by 2030. While this highlights that cyberattacks have a meaningful financial impact, research into the stock market outcomes for firms internationally is sparse. In this study, we use a rich international sample of cyberattacks and privacy violations to assess the market impact of such events, also shedding light on factors that impact the extent of the market outcomes.

This research builds on a rich literature examining the impact of ESG disclosures on the stock market, using this as a proxy for corporate reputational risk [Wong and Zhang, 2022, Capelle-Blancard and Petit, 2019]. Further literature considers the issues of reputational risk emerging from operational risks and company-specific risks, which include cyberattacks and privacy-related violations [Fiordelisi et al., 2014, Sturm, 2013, Gillet et al., 2010]. Linking these two types of literature, the World Economic Forum (WEF) suggest that firms need to start managing such cybersecurity risks as part of their ESG strategy. The WEF view cybersecurity risks as a threat to society more broadly. In this sense, our focus in this research is on an important aspect of the social component of ESG, an area that has received less attention in the academic literature than environmental or governance risks. Our contributions to the literature are numerous. We focus on the novel corporate effects of reputational risk emerging from cyberattacks and privacy-related violations. Our dataset consists of an international panel of cybersecurity risks, with significant additional granularity relative to the extant literature, providing insights in relation to whether the event is classified by media outlets as being severe or whether the information source has considerable reach. This allows us to infer whether media perception of the cybersecurity event influences the stock market outcome for the firm. Finally, we also relate these stock market outcomes to company-specific characteristics, providing a fundamental understanding of the drivers of stock returns emanating from reputational risk.

Several distinct research questions are posited in the following research. Primarily, we investigate how financial markets respond to cyberattacks and privacy violations. Within the context of the novel, collated data obtained from RepRisk, we provide answers to these research questions using stock returns around the specific time the news about cyber breaches is released to the public in the media. Using such data, we can investigate several novel research questions, such as whether the magnitude or reach of a cyber event significantly materially affects market reactions or how inherent

corporate attributes like financial robustness and operational consistency affect market reactions to cyber incidents. We further expand our investigation to analyse whether market reactions are more pronounced for firms experiencing their first major cyber incident when compared to repeat offenders and how the severity, reach, and recurrence of cyber incidents influence the financial market's sensitivity to these events. Placebo tests are used to provide associated methodological robustness. In a secondary analysis, we investigate what role corporate characteristics, such as financial health and operational stability, play when explaining market reactions to cyber-attacks and privacy violations.

As digital transformation continues to drive even more substantial economic progress, understanding financial market reactions to cyber incidents becomes evermore important. Cyber attacks and privacy breaches affect operational integrity and can profoundly impact investor sentiment, reflecting broader economic implications. A clear understanding of the associated financial market reaction to such events leaves policymakers and stakeholders ill-prepared, thereby exacerbating financial volatility. Moreover, as large multinational companies increasingly rely on data and digital transactions for operational purposes, their respective cybersecurity infrastructures indirectly shape broad economic stability. This research provides invaluable insights into the potential financial market effects of such cyber incidents, where furthering our understanding supports improved forecasting and stress testing abilities while underpinning the design of responsive financial regulations and corporate strategies. Hence, this study offers timely insights for policymakers, investors, and corporate leaders, underscoring the intertwined nature of cybersecurity and economic stability.

Through the use of an EGARCH-estimated methodological structure, adapted to account for international effects, return differentials reveal a pronounced negative stock market reaction in the aftermath of cyber attack and privacy violation incidents as identified and collated through the use of a novel database focusing on several spate factors contained within media releases. Average returns are found to have diminished by -0.24% shortly after the analysed events but, interestingly, rebounded to pre-event levels around ten days thereafter. Companies directly involved in these cyber incidents see a discernible decline in returns, while those indirectly associated experience a decrease in returns, albeit to a lesser extent. The market's reaction varies depending on factors such as the nature of the association, severity, reach, and recurrence of these cyber events. Our analysis demonstrates an increasing depth of negative market response over time, suggesting an intensifying financial market sensitivity to cyber risks. The secondary phase of our examination identifies that larger firms face more pronounced market repercussions following cyber indiscretions. Furthermore, corporations that are experiencing such novel events for the first time present significantly more pronounced negative interactions with volatility, credit ranking and credit volatility when compared

to repeat offenders. While novel cyber incidents may cast doubt on a corporation's ability to protect digital assets, repeat occurrences may be perceived as evidence of crisis management expertise. Over time, these recurrent events may become a 'known' risk, dulling market sensitivity to their adverse effects. Such repetition may also diminish information asymmetry, allowing for a more informed understanding of a company's cyber vulnerabilities, resulting in more measured market reactions. Critically, we found that the market's reaction is not significantly swayed by the cyber event's magnitude or spread but emphasises the implicated firms' inherent attributes.

This research highlights key policy and regulatory recommendations when confronting growing challenges sourced in cyber attacks and privacy violations. Strong market responses to cyber events indicate a need for thorough regulations to advance cyber risk reporting, particularly for larger enterprises. Differences in market reactions, influenced by company specifics, further suggest the necessity for industry-tailored guidance addressing distinct risks. Additionally, the market's differential response to novel cyber events underlines the priority of enhancing cyber safeguards for firms not previously nor those indirectly affected while promoting clear communication universally. Results support a proactive approach combining timely cyber oversight, regular risk evaluations, and open reporting, ensuring firms and investors navigate our evolving cyber threats collaboratively.

The rest of this paper proceeds as follows: Section 2 provides a concise overview of previous literature on cyberattacks and privacy violations, with further empirical evidence to underpin the research questions and methodological processes used to analyse. Section 3 provides a thorough explanation of the data and methodologies employed, while Section 4 summarises the key results identified. Section 5 provides an overview of the relevant discussion relating to the results, the key policy and regulatory implications, and several directions for future research. Finally, Section 6 concludes.

2. Previous Literature

Kamiya et al. [2021] showed that if a successful cyberattack leads to the compromise of personal financial data, there is a notable decline in shareholder wealth, surpassing the direct costs of the attack. This additional loss is more substantial when the attack leads to a greater reduction in sales growth, and it is mitigated when the company's board prioritises risk management before the attack. They also indicate that the aftermath of an attack prompts the company to enhance its risk management and information technology while diminishing the motivation for managerial risk-taking. Ultimately, successful cyberattacks adversely influence the stock price of companies within the same industry as the targeted firm. Further, Florackis et al. [2023] introduced an innovative way to gauge cybersecurity risk for all US-listed companies at the firm level by utilising textual analysis

and comparing firms that experienced cyberattacks and those that did not. They subsequently investigate whether the degree of cybersecurity risk affects stock returns across various firms. They show that portfolios of companies facing significant cybersecurity risk tend to outperform their counterparts, demonstrating an average annual out-performance of up to 8.3%. However, such high-exposure firms exhibit weaker performance during periods of heightened cybersecurity risk. Crosignani et al. [2023] investigate the supply chain consequences of the most severe cyberattack recorded to date. They show that the attack's impact extended beyond the targeted firms to their clients, resulting in a quadrupling of the initial profit decline. Companies managed to navigate this disruption by relying on internal financial reserves and increased borrowing, primarily through bank credit lines.

Related literature has, by assessing the impact on stock returns, examined the reputational risk from operational loss events in financial services. These company-specific news announcements relate to failures in systems, policies and processes that disrupt the operation of the business. Sturm [2013] provides evidence of negative announcement returns after the first media coverage of the operational loss event. While an assessment of different operational risk types is reported, cybersecurity breaches are not examined in isolation. Gillet et al. [2010], using a sample of 154 events, also reported negative returns and increased trading volume after the announcement of operational losses. Similar to Sturm [2013], events are broken out into internal fraud, client products, and business practises, but with no focus on cyber-derived risks. Finally, Fiordelisi et al. [2014] find similar evidence for negative announcement day returns in the financial industry and event types are focused on broad categories. Our work differs from this literature by the focus on cyberattacks and privacy-related violations across a broad range of industries rather than focusing on banks and financial institutions.

Recent research has leveraged the RepRisk database to explore the multifaceted dimensions of Environmental, Social and Governance (ESG), Corporate Social Responsibility (CSR) and other significant corporate reputational disasters, revealing critical insights into corporate behaviours and their societal implications. Many studies consistently emphasise the importance of transparency and disclosure in managing ESG and CSR controversies [Friedman and Miles, 2001], converging on the understanding that ESG disclosure can influence analysts' perceptions, moderate forecast errors, and even reshape firm reputations and the outside perception of risk [Kumarasiri and Gunasekarage, 2017, Bouslah et al., 2018, Moll and Yigitbasioglu, 2019]. Furthermore, biases in ESG controversies data, especially regarding media source selection, highlight the challenges and trade-offs firms and investors face in comprehensively assessing corporate behaviour. Evidence of the elevated usage of ESG-related databases such as RepRisk has also been observed recently. Wang

and Li [2019] utilised RepRisk-collated data to examine how corporate social irresponsibility (CSI) disclosures impact multinational companies' reputations and the strategic use of foreign subsidiary governance in response, highlighting divergent functions of information and ownership control and the influence of host-country press freedom and regulatory quality. Li and Wu [2020] used RepRisk data between 2007 and 2015 to assess firm-level ESG impact and CSR engagements, finding private firms reduce negative ESG incidents post-United Nations Global Compact (UNGC) involvement, whereas public firms often decouple CSR actions, with shareholder-stakeholder conflicts, ownership type, and ESG incident type as key influencers. Gualandris et al. [2021] used Bloomberg SPLC data while controlling for industry-level reputational risk using RepRisk for 4,803 firms across 187 supply chains in an attempt to investigate how supply chain structure affects transparency, revealing positive associations with supply chain density and geographical heterogeneity but a negative link with clustering, while Schiemann and Tietmeyer [2022] examined 8,369 firm-year observations to find ESG controversies increase analyst forecast errors, but ESG disclosure moderates this effect, with social controversies and disclosure being most influential.

3. Data and Methodology

Data based on events relating to cyberattacks and privacy violations are obtained from the RepRisk database,[1] which has been used in research to date that has focused on transparency, corporate social responsibility, and investigation of ESG-focused issues, amongst other areas [Akyildirim et al., 2020]. Data is obtained along with several related characteristics, presenting specific analysis as to the severity, novelty, and reach of the reputational event. Within the RepRisk database, each risk incident is analysed according to three parameters: 1) Severity constitutes the harshness of the risk incident or criticism. The severity is determined as a function of three dimensions: firstly, what are the consequences of the risk incident (e.g., with respect to health and safety: no further consequences, injury, death); secondly, what is the extent of the impact (e.g., one person, a group of people, a large number of people); and thirdly, was the risk incident caused by an accident, by negligence, or intent, or even in a systematic way. There are three levels of sever-

[1] RepRisk is a global leader and pioneer in data science, specialising in premium ESG and business conduct risk research and quantitative solutions. Since 2006, RepRisk has been leveraging the combination of AI and machine learning with human intelligence to translate big data into actionable research, analytics, and risk metrics. With daily-updated data synthesised in 23 languages using a rules-based methodology, RepRisk systematically flags and monitors material ESG risks and violations of international standards that can have reputational, compliance, and financial impacts on a company. The RepRisk ESG Risk Platform is the world's largest database, covering 200,000+ public and private companies and 50,000+ infrastructure projects of all sizes in every sector and market. Leading organisations around the world rely on RepRisk as their key due diligence solution to prevent and mitigate ESG and business conduct risks related to their operations, business relationships, and investments.

ity: low severity, medium severity, and high severity; 2) Reach of the information source (influence based on readership/circulation as well as by its importance in a specific country), according to RepRisk's own rating. All sources are pre-classified by reach: limited reach, medium reach, and high reach. Limited reach sources 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. The few truly global media outlets are high-reach sources; and 3) novelty (newness) of the issues addressed for the company and/or project, whether it is the first time a company/project is exposed to a specific ESG issue in a specific location. RepRisk data is obtained between 1 January 2011 and 31 December 2022, resulting in 1,716 observations. The frequencies of the included ESG events are presented in Figure 1, with evidence of significant growth of cyberattacks and privacy violations evident since 2018.

Insert Figure 1 about here

RepRisk has a structured framework of 28 core ESG issues that drive their research process. These issues are comprehensive and mutually exclusive, forming the foundation for linking and categorising risk incidents within their dataset. This framework helps ensure that every risk incident is associated with at least one of these 28 ESG issues. Additionally, RepRisk extends its coverage with 73 Topic Tags, which are specific and thematic categories related to ESG "hot topics" and emerging trends. Each Topic Tag can be linked to multiple ESG issues, providing a dynamic and flexible way to capture and analyse various dimensions of ESG risks and opportunities.

One of the ESG hot topics among RepRisk Topic Tags is Cyberattack. It is defined as a premeditated infiltration of computer systems, technology-based businesses, and networks. A cyberattack is a deliberate and premeditated attempt to breach the security of computer systems, technology-based businesses, and networks for various malicious purposes. These attacks can involve unauthorised access, theft, manipulation, or destruction of digital information and resources. Cyberattacks can target individuals, organisations, governments, and even critical infrastructure, with the intention of causing harm, extracting valuable data, disrupting operations, or gaining control over systems.[2] Another topic tag of particular interest in the same framework is privacy violations. It is defined as

[2]For example, one of the cyberattack incidents identified by RepRisk on September 7, 2017, is for the US-based consumer credit reporting agency Equifax. Indeed, on this day, Equifax announced that a cyber-attack on its computer systems between May and July 2017 had enabled hackers to access the personal data of about 143 million people in the US. By September 21, Equifax shares had plummeted by 33 percent following reports that the cybercriminals had been able to access full names, social security numbers, birth dates, and addresses, allegedly leaving consumers vulnerable to identity theft.

actions by a company that result in the unauthorised access or distribution of an individual's personal information without their permission or knowledge. It commonly occurs through indirectly failing to protect privacy, i.e. outside data hacking and loss of client info, or directly violating privacy, such as phone or account hacking by a company or the sale or release of confidential client info. Indeed, privacy violations refer to instances where an individual's personal information, data, or rights to privacy are compromised or infringed upon without their consent. These violations can occur in various contexts, such as online interactions, data breaches, surveillance, or unauthorised sharing of personal information. Privacy violations can have significant consequences for individuals, including loss of control over their personal data, potential identity theft, and erosion of their fundamental right to privacy.[3]

Insert Table 1 about here

To investigate the effects of cyberattack and privacy violation events upon corporate returns, we first proceed to match events identified from the RepRisk database with each identified ISIN code, where stock data is obtained for the period 1 January 2010 through 30 June 2023. Summary statistics relating to each country analysed are presented in Table 1.[4] We next calculate the natural logarithm of returns as $R_{i,t} = ln\frac{P_{i,t}}{P_{i,t-1}}$. It is well-documented in the literature that the standard tests to measure the effect of a specific event on stock prices must be modified due to the presence of heteroskedasticity [Engle, 1982, Bollerslev, 1986]. Therefore we consider various options within the Generalised Autoregressive Conditional Heteroskedastic (GARCH) family models to best understand the influence of cyberattacks and privacy violation events. We employ an exponential generalized autoregressive conditional heteroscedasticity (EGARCH) model developed by Nelson [1991] to specify the conditional variance (h_t) of the innovations.[5] The EGARCH model

[3]For example, one of the privacy violations identified by RepRisk on January 10, 2014, is for the US luxury retailer Neiman Marcus Group. Indeed, on this day, Neiman Marcus disclosed that it had been a victim of a major data privacy breach. According to the US Secret Service, the websites of over 1,000 US retailers were hacked by criminal gangs operating from Eastern Europe. There were fears that the attacks had compromised the companies' customer credit and debit card information following suspicions that malware had been installed in in-store payment systems.

[4]Stock market data selection was considered within the context of providing a strong sample of data both before and after the events identified and collated through the RepRisk database. Therefore, extended stock market data is obtained to generate a strong sample period of analysis to provide an adequate representation of stock market behaviour both before and after the earliest and latest events recorded in our sample.

[5]EGARCH exploits information contained in realised measures of volatility while providing a flexible leverage function that accounts for return-volatility dependence. While remaining in a GARCH-like modelling framework and estimation convenience, the model allows independent return and volatility shock. This dual shock nature leaves room for establishing a variance risk premium. In our selection, other competitive models included EGARCH, TGARCH, Asymmetric Power ARCH (APARCH), Component GARCH (CGARCH) and the Asymmetric Component GARCH (ACGARCH). The optimal model is chosen according to three information criteria, namely the Akaike (AIC), Bayesian (BIC) and Hannan-Quinn (HQ).

has the advantage of ensuring the positivity of estimated conditional variance without any parameter restrictions, in contrast to the alternative GARCH specifications. It also imposes fewer parameter restrictions to guarantee the stationarity of the conditional variance. We focus specifically on both the return and volatility of each company through the use of an EGARCH(1,1) methodology, which was selected based upon several goodness-of-fit testing procedures. We utilise the mean equation of the EGARCH(1,1) methodology as displayed in Equation (1).

$$r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t, \tag{1}$$

while we express the variance equation of our EGARCH(1,1) model as follows:

$$\ln(h_t^2) = \omega + \alpha\varepsilon_{t-1} + \gamma(|\varepsilon_{t-1}| - E(|\varepsilon_{t-1}|)) + \beta \ln(h_{t-1}^2). \tag{2}$$

We include an additional d_t term in Equation (1) in our analysis to provide a coefficient relating to the observed return differential for each of our investigated cyberattack and privacy violation events. The volatility sourced within shocks incorporated in the returns of traditional financial markets is therefore considered in the volatility estimation of the selected structure. Equation (1), r_{t-1} and r_{t-2} represent the lagged values of the observed corporate returns, while I_t represents the returns of the respective international benchmark index upon which the stock is traded and represents the interaction between the selected company returns and the corresponding domestic market index. To adequately and robustly assess the time period surrounding each event, we measure abnormal returns using multiple estimation windows of three months around each identified event, which is assumed to occur at t_0, across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur as per Akyildirim et al. [2020], Corbet et al. [2020], Meegan et al. [2021]. Multiple other variations of analysis windows were considered; however, for the brevity of the presentation, only those listed above were included. Each number refers to the specific trading days relative to each identified event. Specifically, the periods [0,+20] and [0,+60] reflect return differentials for the periods one and three months after each identified event, reflecting the persistence of both returns and volatility in the aftermath of each event. Methodological structures are then repeated based on the characteristics being analysed as to whether the results have been influenced by incident severity, reach, novelty, or whether the event is directly (sharp) or indirectly (unsharp) related to each company. Further testing is conducted based on the year and geographical region in which the analysed event occurred. In total, 77,220 EGARCH methodologies are analysed, considering nine windows of analysis surrounding the

1,716 analysed events and the multiple robustness procedures considered through placebo tests.

To provide additional methodological robustness, testing procedures are again considered using the same identified companies and methodological structure. However, the windows analysed are re-considered when progressing three, six, nine, and twelve months into the future for a group known as the placebo group hereafter. As no cyberattack or security breach is found to have occurred on these dates, there should theoretically exist no significant market response for this precise reason. Considering all of the events, it would be anticipated that each of these further analysed placebo group windows should generate no significant effect, therefore verifying the methodological selection provided.[6]

To provide additional explanatory value, the presented return differentials resulting from the RepRisk-defined cyberattack and privacy violations are then considered in a methodology that encapsulates several distinct corporate characteristics. Each selected variable has been considered for various reasons, primarily surrounding the many industrial and sectoral pressures that exist, to identify whether deteriorating financial performance can be observed as an explanatory factor when considering the financial market response to such significant breaches. The data considered include Revenue Surprise[7], the natural logarithm of company market capitalisation, the Credit Combined Global Rank[8], the twelve-month Volatility Rank[9], and finally, the Credit Structural Asset Volatility Global Rank[10]. We consider the result surrounding the event window $[t_0,+1]$ to test whether corporate characteristics can explain whether such differential stock market response diminishes or perhaps persists in varying manners due to corporate factors.[11]

[6]Due to the large number of additional results generated through this additional robustness testing procedure, only those results focusing on the six-month window are considered hereafter for the brevity of presentation. All other results pertaining to these additional robustness testing procedures are available from the authors upon request.

[7]Each of these variables is estimated as the difference between the actual value and the mean analyst estimate expressed as a percentage (as obtained from StarMine SmartEstimates through the Thomson Reuters DataStream data package).

[8]The variables represent the current global level 1 through 100 percentile rank respectively of a company's 1-year default probability based on the StarMine Combined Credit Risk Model, which blends the Structural, SmartRatios and Text Mining Credit Risk models into one final estimate of credit risk at the company level. Higher scores indicate companies that are less likely to go bankrupt or default on their debt obligations within the next 1-year period.

[9]Estimated as the current 1 through 100 percentile rank of the security versus all other securities on trailing twelve-month volatility.

[10]Estimated as the current global 1 through 100 ranks of the annualised volatility of the market value of the firm's assets according to the Structural Credit Risk Model. Firms with higher values of asset volatility are more likely to cross their default point (hence perceived to be more risky) and receive lower rank values.

[11]All examined windows of analysis were considered in this secondary analysis; however, for the brevity of presentation, only event window $[t_0,+1]$ are presented. All other results are available from the authors upon request.

4. Results

Methodological robustness is provided when considering Table 2, representing the associated summary statistics based on the EGARCH-estimated return differentials due to cyberattacks and privacy violations. A distinct trough of internationally-adjusted returns is identified through windows (-5,-1), (t_0,+1), (t_0,+5) and (t_0,+10), indicative of a short, sharp shock to the analysed corporations in the days surrounding media release of news relating to cyberattack and privacy violations. At window (t_0,+1), average returns are found to have fallen by -0.24% across all events analysed before quickly reverting around ten days post-event to levels comparable to those observed in the period before. Such stock market response is found to be associated with a short sharp elevation in variance (+0.0003), extended negative skewness of returns (-4.67), and a significant increase in kurtosis (+37.46). When considering the estimated percentiles of EGARCH-estimated return differentials, there is a notable deterioration and elevation of the lowest and highest returns, respectively. Most notably, when considering the 1% percentile, during the window (-60,-1), the internationally-adjusted return differential is estimated to be -0.96%; however, during the window (t_0,+1), such returns deteriorate to -6.01% in the most extreme circumstance. When considering the presented placebo group analysis, based on the same corporations with each dummy variable presented six months after the actual cyberattack and privacy violation date, no significant differential of pricing behaviour is identifiable, indicating that the selected sample and methodological selection correctly segregate the considered event. Results are further verified visually in Figure 2, where clear differential behaviour between the primary and placebo groupings are presented.

Insert Table 2 & Figure 2 about here

Such EGARCH-estimated return differentials are then considered with regard to several RepRisk-defined characteristics such as event sharpness, severity, reach and novelty in Tables 3 through 6, respectively. In Table 3, we identify return differentials associated with event sharpness, that is, where the sharp events are associated directly with the company, whereas unsharp events are incidents where the corporation is mentioned in the news article, yet the criticism is defined as complex, or not precisely defined. Significant return differentials are identified, where direct, sharp events are associated with a moderate discount; however, in both analysed groups, returns are found to become significantly negative during window [t_0,+1] by -0.25% and -0.20%, respectively. The analysed placebo grouping presents no evidence of significant interactions, indicating strong methodological robustness. It is particularly interesting to note that irrespective of direct or indirect exposure to

cyberattacks and privacy violations, financial market investors appear apathetic to the corporate's role in such exposure, only that its defensive ability has been brought into disrepute.

Insert Tables 3 & 4 about here

Focusing on the severity of respective cyberattacks and privacy violation incidents, Table 4 provides several interesting observations. Severity is determined as a function of the alleged violation of national laws and international standards along multiple dimensions, where more significant breaches are found to be associated with more significantly negative internationally-adjusted returns (-0.32%) when compared to those of a lower severity (-0.24%). Further, results remain more persistently negative in more severe cases analysed, where returns are found to be significantly negative in the one and two-week periods thereafter (where returns are estimated to be -0.34% and -0.22% respectively). In Table 5, we observe the results separated by event reach, where broad reach encapsulates high-reach international news sources, while narrow reach accounts for both low- and medium-reach news sources. Low-reach sources include local media, smaller NGOs, local governmental bodies, blogs, and internet sites. Results indicate little differential in the short-term response associated with cyberattacks and privacy breaches; however, differential behaviour with regard to persistence is identified. Specifically, while broad-reaching news events generate significant negative returns in window $[t_0,1]$ of -0.22%, such negative returns are found to persist for one and three months thereafter (-0.08% and -0.05% respectively). However, low-reach violations generate a sharp negative shock (-0.19%) of a substantially shorter duration. In both event severity and reach analyses, associated placebo testing procedures verify the methodological selection.

Insert Table 5 about here

Event novelty corresponds with the 'newness' of the event, whether it is a new event experienced by the company or a re-occurring issue. In Table 6, we observe that repeat offenders experience more significantly depressed returns (-0.29%) than those companies experiencing such cyberattacks and privacy violations for the first time (-0.16%). Results persist for both samples, while associated placebo testing procedures verify methodological selection due to the non-identification of any significant events.

Insert Table 6 about here

When considering the time of occurrence of such events, we repeat our respective analyses as separated by the year of occurrence in Table 7 with associated placebo testing procedures supporting our methodological selection presented in Table 8. Results indicate that there existed no significant internationally-adjusted market impact before 2016; however, in the period thereafter, each year has presented evidence of sharp negative price effects during the immediate event window $[t_0,+1]$ following each event. Results are found to become strongly persistently negative in 2016, 2017, and 2022 with evidence of negative effects lasting up to one month thereafter.

Insert Table 7 & 8 about here

When attempting to understand whether corporate characteristics can further explain such differential responses, several distinct observations can be made. Based on the entire sample and focusing on the event window $[t_0,+1]$ due to the multiple significant negative outcomes identified during the EGARCH-estimated return differential analyses, as presented in Table 9, we identify that larger corporations are broadly associated with more positive outcomes in the aftermath of cyberattacks and privacy violations. It would appear that larger corporations are perceived to be more stable, robust, and capable of resolving issues pertaining to such incidents, verifying multiple previous studies that identified a link between corporate size and technological resilience [Corbet and Gurdgiev, 2019]. In quite a distinct result, revenue surprise is associated with a significant negative stock market response in each analysed methodological specification (-1.29% and -1.11%, respectively). A revenue surprise and a cyberattack or privacy violation intensify negative stock market responses due to heightened uncertainties. The unexpected revenue data can sow doubts about the company's stability, and when combined with a security breach, the uncertainty compounds. Such surprises might make investors sceptical about the management's forecasting reliability and capacity to manage crises transparently. It may also spotlight operational vulnerabilities, with a cyber incident underscoring this perception. Moreover, the financial aftermath of cyber breaches, such as fines and reputational harm, may heighten concerns if the firm's revenues are unpredictable. Consequently, investors could reevaluate the company's risk, lowering stock prices. This is exacerbated by market momentum, where consistent negative news intensifies adverse reactions.

Insert Table 9 about here

Such interaction with revenue surprise also corresponds with negative interactions with the variables corresponding to twelve-month corporate volatility ranking (-0.22%) and corresponding Credit

Structural Asset Volatility Global Rank (-0.22%) and Credit Combined Global Rank (-0.13%). Each variable represents a distinct dynamic of recent corporate performance alongside several metrics that encapsulate financial market expectations of future financial performance. Associated placebo testing procedures are presented alongside the results of the corresponding secondary analyses based on the event window $[t_0,+1]$ six months after each event, thus determining an expectation of no significant outcome, which is identified in the associated results thereby further verifying methodological selection. Companies with high corporate volatility rankings are inherently perceived as high-risk investments, and this perception intensifies in the wake of major cyberattacks or privacy breaches. This existing volatility, representative of potential unpredictability in future earnings, becomes even more magnified when paired with the uncertainty cyber incidents introduce. Combining these factors can drive institutional investors to reconsider their positions, possibly pushing them beyond risk tolerance and prompting divestment. This environment can also compound existing questions surrounding management ability while pre-existing volatility can signal liquidity concerns, making any direct or indirect costs from cyber incidents even more concerning. Given that such firms are under heightened scrutiny, any negative event, such as a cyberattack, can exacerbate reputational damage, leading to significant market reactions. Similarly, the Credit Structural Asset Volatility (CSAV) Global Rank offers insight into a firm's asset value fluctuations, a key determinant in assessing credit risk. Companies with high CSAV rankings indicate pronounced asset volatility, making the stock market response to cyberattacks or privacy breaches especially adverse. This heightened volatility, besides indicating creditworthiness concerns, particularly post-incident costs, can also lead to apprehensions about the company's solvency and liquidity. Investors tend to monitor such high CSAV-ranked firms, making them particularly susceptible to reputational decline following significant negative events. The synergy of significant asset volatility and cyber incidents can erode investor confidence and increase market uncertainty; driving pronounced downturns.

Insert Table 10 about here

We further extend this exploratory analysis to investigate whether such effects correspond with distinct differentials as determined by event sharpness, severity, reach and novelty as presented in Tables 10 through 13, respectively. In Table 10, it is apparent that only corporations directly linked with cyberattacks and privacy violations present interactive effects with prior corporate characteristics and risk perception. Those corporations indirectly identified do not present evidence of such interaction, verifying the limited exposure earlier identified. When corporations are directly implicated in cyberattacks and privacy violations, their prior corporate characteristics, such as

financial health, operational stability, or management competence, interact with the risk perceptions generated by these events. The direct involvement in a cyber event underscores and perhaps magnifies the existing perceptions about the company, leading to more pronounced market reactions. On the other hand, corporations that are indirectly identified or associated with cyberattacks and privacy violations do not show this same level of interaction. Their tangential or secondary involvement does not draw international focus on their corporate characteristics similarly. The limited exposure noted for indirectly identified corporations confirms that the market's primary focus and concern lie with the main actors in these incidents.

Insert Tables 11 & 12 about here

No discernible differentials are identified when separating the groups by severity and reach, as presented in Tables 11 and 12, respectively, indicating that corporate characteristics provide explanatory value irrespective of whether the cyberattack or privacy violation is large or small.

Insert Table 13 about here

When considering event novelty in Table 13, it is evident that corporations that are experiencing such novel events for the first time present significantly more pronounced negative interactions with volatility, credit ranking and credit volatility when compared to repeat-offenders. When corporations face cyberattacks or privacy violations for the first time, the unexpected nature can catch investors off guard, amplifying negative sentiment and causing a pronounced adverse market reaction. This is often compounded by financial indicators like volatility or credit rankings. Conversely, repeat offenders may have developed improved response mechanisms, communication strategies, or remediation processes from past experiences, thereby reducing the negative market response. While corporations experiencing such events for the first time may face doubts about management's ability to safeguard digital assets, repeat offenders might be seen as having gained expertise in handling such crises. Over time, repeat events can lead investors to consider cyber incidents a 'known' risk, desensitising the market to their negative effects. Finally, repeat events may reduce information asymmetry, giving markets more complete information about a company's cyber risks and technological ability, leading to more calibrated reactions. In all samples analysed, placebo groupings correspond with no significant effects, thereby providing significant methodological robustness.

5. Related Discussion and Directions for Future Research

The robust findings presented herein underscore the intricate relationship between cyber vulnerabilities and their consequential financial repercussions. Corporate digital transformation has propelled cyber risks to the forefront of corporate concerns, and a nuanced understanding of their economic implications is paramount. For market participants, regulators, and policymakers alike, these results offer several significant interactions that display the ever-changing dynamism of the financial market's sensitivity to technological threats. Not only does this research present evidence of the immediate stock market reactions post-cyber-attacks and privacy violations, but it also presents evidence surrounding broader macroeconomic effects, each of which is potentially capable of destabilising sectors, or even entire economies, in the advent of large-scale cyber incidents. A key result from this analysis surrounds the nuanced differentiation that financial markets consider between corporations directly implicated in cyber attacks and privacy violations and their indirectly associated counterparts. Such discernment presents substantial evidence surrounding the sophistication of financial market informational efficiency when delineating responsibility and culpability. This suggests a heightened need for corporations to bolster their technological defences and communication strategies, ensuring that their roles in any cyber incident are transparently conveyed to prevent unnecessary reputational collapse.

Results indicating that financial markets have become progressively sensitive to cyber risks over time are particularly interesting, where this evolving trend warrants further scrutiny into whether such heightened sensitivity stems from a growing understanding and awareness of cyber risks or if it is indicative of the increasing dependence of corporations on digital infrastructures, thereby magnifying the potential fallout from digital breaches. Moreover, the relatively uniform market responses, irrespective of incident severity, present intriguing implications, emphasising a crucial aspect for corporations; that their inherent resilience, transparency, and operational fortitude may significantly outweigh external threats in shaping market perceptions.

Our findings also have multiple implications regarding the relationships between corporate characteristics and corporate stock resilience when considering portfolio construction procedures and diversification strategies relating to ESG. One critical step in the portfolio selection and construction process is qualitative screening and selecting eligible stocks into ad-hoc ESG-oriented portfolios with clear goals, often incorporating substantial corporate resilience against risks associated with unethical and unlawful activities. An analogue of such a step is the well-known Shariah screening standards used by some main index providers, such as S&P, Dow Jones, MSCI and FTSE, amongst others, when compiling ethical or religious-based portfolios. Under such standards, firms with substantial revenue derived from illicit businesses or activities are filtered out [Abdelsalam et al., 2023].

As a result, one can expect that the portfolio will be protected against the potential shocks of unethical behaviour. Similarly, some of the results in this research can contribute to the screening task of selecting adequate stocks for ESG-featured portfolios with a target of strong resilience to shocks of cyberattacks and privacy violations. For instance, firms with higher market capitalisation, lower volatility, lower credit volatility rank, and more abundant experience in handling events of cyberattacks and privacy violations possess higher corporate resilience. Therefore, such stocks can be considered appropriate candidates in the screening procedure. Hence, the findings shed light on portfolio diversification strategies when ESG is factored in.

Several policy implications extend from the presented results, presenting evidence of nuanced inter-dynamics between cyberattacks and privacy violations and that of corporate financial performance, where such responses are significantly interconnected with existing corporate characteristics, reflecting the significance of a firm's financial stability, management performance, and operational integrity. Governments and policymakers could focus on the role of cyber resilience as an essential economic tool, investing further in robust national and sectoral cyber infrastructures and collaborating with international counterparts to develop consistent cross-border cybersecurity standards while reinforcing broad cyberinfrastructure. Policies could focus on implementing mandatory enforcement and uniform disclosure of cyber incidents and data breaches. Such transparency could include standardised reporting formats, periodic assessments, and third-party audits, ensuring that the market reactions are informed by concrete facts rather than speculative uncertainties. Increased focus on multinationals and those companies leveraging from cross-border regulatory disparities should also merit further attention. Beyond reacting to incidents, policies must foster a culture of proactive vigilance within corporations. Incentives for routine internal evaluations, employee training, and partnership with cybersecurity experts could drive businesses to constantly evaluate their cyber-readiness and overall operational health. Improving our understanding that existing corporate characteristics can amplify and dampen market reactions to cyber threats offers valuable insights for policy design. Strategic regulations around financial reporting, risk management, and corporate governance can ensure that firms are resilient to cyber threats and transparent about their inherent risk factors.

From a regulatory standpoint, the findings of this research emphasise the significance of establishing all-encompassing cyber risk assessment frameworks. Such frameworks would not merely act as evaluative tools but standardise how corporations perceive, measure, and report their cyber vulnerabilities. This consistency is key to ensuring that the market receives a unified perspective on cyber risks, irrespective of the size or sector of a firm. Regulatory bodies should recognise the heightened risks associated with cyber-attacks in sectors such as finance, healthcare, and energy

and draft guidelines tailored to the intricacies of these industries, particularly focusing on more rigorous disclosure requirements, frequent risk assessments, and specialised training protocols. Beyond merely reacting to cyber incidents, it is imperative that firms proactively and periodically disclose their cyber readiness and resilience measures. Such transparency bolsters investor confidence and prompts firms to continuously monitor and improve their cybersecurity defences. A standardised reporting format, backed by third-party validation, can further enhance the credibility of these disclosures. Regulation should also address indirect cyber associations, where indirect associations' subtler yet equally potent ramifications necessitate attention. Firms may have muted market reactions not because they are insulated from the risks but possibly due to latent information asymmetries. To address this, regulators could draft stipulations that mandate disclosures about a firm's third-party dependencies, partnerships, and any indirect exposure to cyber threats. As cyber threats evolve, so should regulatory oversight. Continuous dialogue between industry experts, cybersecurity professionals, and regulators will be crucial. This collaborative approach can ensure that the regulatory landscape remains adaptive and robust.

Our research focuses on the short-term financial consequences of cyber breaches, yet the long-term financial implications, potentially persisting for years, remain unexplored. Further research could focus on the corresponding sentiment of social media response to such news announcements, providing a deeper understanding of the inherent market response to such significant corporate reputational incidents and shedding light on the heterogeneous impact of information dissemination. Further questions surround whether firms bear lasting "cyber scarring" that impedes their long-term growth prospects in the aftermath of such incidents or does the market adjust its initial reactions. Understanding the evolution of firms' cybersecurity strategies post-breach within this context could reveal the interplay between proactive adaptability and sustained financial performance. Another pivotal area surrounds the relationship between the spread of cyber incident news, especially through algorithm-driven platforms, and subsequent market reactions. The role of various investors, from retail swayed by mainstream media to institutions wielding advanced analytics, merits attention. Notably, post-2016 market reactions shifted, suggesting broader global changes, perhaps due to evolving cyber awareness or international regulations. Exploring the market's treatment of companies based on their involvement in cyber incidents or how reactions differ among sectors like healthcare and finance and associated sub-sectors such as fintech can offer nuanced insights. Regional factors, spanning cultural values to economic structures, might yield differential market reactions, while industry-specific analyses can reveal unique vulnerabilities. With emerging technologies like quantum computing and the growing influence of artificial intelligence presenting new cyber challenges, gauging the market's readiness for such breaches becomes essential. Overall,

the interplay between cyber risks, financial markets, and technological evolution opens vast avenues for further academic exploration, with our study offering a foundational perspective in navigating this digitalised economic landscape.

6. Conclusions

Assessing the market responses to cyberattacks and privacy violations, our research sheds light on the nuanced interplay between technological vulnerabilities and economic consequences. Through the presented EGARCH estimated return differentials, this research unveils significant negative stock market reactions to cyber-attacks and privacy violations, as quantified through a novel dataset that collates and ranks the scale of media coverage that ensues each respective event. The presented analysis uncovers a significant, pronounced decrease in internationally adjusted returns around the time of cyberattack and privacy violation news. Specifically, the days surrounding these events see a decline, with average returns dropping by -0.25% shortly after the event. Interestingly, this negative trend is quite short-lived, with returns rebounding to approximate pre-event levels around ten days post-event. The elevated variance and extended negative skewness observed in returns might reflect heightened investor uncertainty and risk perception, leading to erratic market behaviour and elevated short-term financial market volatility.

Companies directly implicated in cyber incidents face more immediate consequences, experiencing a discernible return discount. This could be attributed to a direct attribution of responsibility, impacting investor confidence. However, the differentiation between direct and indirect associations seems marginal, with both analysed groups experiencing decreased returns. Financial market investors appear less concerned with the nature of the association and more with the mere fact that a company's cybersecurity defences have been challenged or breached. The results present evidence of an intuitive correlation between the severity of an incident and its market impact. Breaches of national and international standards, arguably perceived as more egregious, are penalised more severely by the market, leading to steeper declines in returns. This underscores the market's sensitivity to not just the occurrence but also the magnitude of a violation.

Furthermore, the reach of the event news plays a pivotal role. Broad-reaching, pervasive events sustain their negative influence for extended periods. On the other hand, incidents reported by low-reach sources induce a more transient impact, possibly due to limited exposure and dissemination of such news. Recurring offenders bear the brunt of repeated lapses, suffering from more pronounced return declines, hinting at the market's dwindling patience and tolerance for repeat misdemeanours. Companies encountering their first major cyber incident face penalties, which are milder than repeat offenders. This suggests that the market might be more forgiving of isolated lapses but less so of

patterns of negligence. A time trend emerges from the data. Before 2016, cyber incidents appeared less consequential in their market impact. However, post-2016, a clear pattern of negative price effects emerged, most notably in 2016, 2017, and 2022. This could reflect a growing awareness and understanding of cyber risks over time, coupled with increasing expectations of corporate cyber resilience in more recent years. In essence, the market reacts variably to cyberattacks and privacy violations, influenced by factors such as the directness of association, the severity, reach, and recurrence of incidents. The growing depth of negative market response suggests that the financial market's sensitivity to cyber risks intensifies as the digital era progresses. Associated robustness testing procedures verify methodological selection processes, where investigated placebo groups present no significant financial market interaction.

The secondary phase of our analysis emphasises the explanation of the market reactions through the lens of corporate characteristics. These reactions are more pronounced for larger firms, suggesting that market participants weigh the implications of such incidents differently based on the corporate size, thereby confirming previous studies that linked corporate magnitude to technological resilience. Interestingly, instances of revenue surprises were found to amplify this negative market response considerably. Such revelations underscore the heightened uncertainties from unexpected revenue data compounded with cyber incidents, leading investors to question the reliability of management's forecasting and the firm's overall stability. Further, we identified that companies with high twelve-month corporate volatility rankings experience intensified adverse reactions after major cyber-attacks or privacy breaches. This existing volatility, denoting potential unpredictability in future earnings, is exacerbated by the uncertainties that cyber incidents introduce. Similarly, the Credit Structural Asset Volatility Global Rank, which provides insights into a firm's asset value fluctuations, became a pivotal determinant in shaping stock market responses post-cyberattacks. Firms with pronounced asset volatility have especially negative responses, spotlighting investor concerns about creditworthiness, solvency, and liquidity in a post-cyberattack landscape.

Furthermore, we investigate the relationship between cyberattacks, privacy violations, and corporate characteristics, further revealing nuanced market reactions contingent on these dynamics. The research decisively underscores that corporations directly embroiled in cyber indiscretions bear pronounced market repercussions, potentially magnified by their antecedent corporate attributes, such as financial robustness and operational consistency. Such a result underscores the financial market's discerning ability to differentiate between primary actors and those tangentially associated, with the latter experiencing a markedly subdued response, evidencing the market's focal attention on primary culpable entities. Moreover, when analysing the results as separated by the dimensions of incident severity and reach, the findings proffer an intriguing outcome where the magnitude or

spread of the cyber event doesn't substantially delineate market reactions. This indicates a market perspective that primarily emphasises the implicated corporations' inherent attributes over the cyber incident's dimensions, suggesting that markets may weigh inherent corporate resilience and competence over the scale of external threats. In the context of event novelty, the study demonstrates that corporations that are experiencing such cyber-attacks and privacy violations for the first time present significantly more pronounced negative interactions with volatility, credit ranking and credit volatility when compared to repeat-offenders, who witness a more moderated reaction, possibly due to the development of response strategies or market desensitisation. This may point to a market learning curve where repeat occurrences provide incremental insights into a corporation's cyber risks and technological abilities, culminating in more tempered reactions. Moreover, the intertwined relationships uncovered between corporate characteristics and stock resilience to cyberattacks and privacy violations shed light on portfolio diversification strategies focusing on superior profile desensitised to ESG-related risks. Specifically, corporate characteristics contributing to strong resilience can be factored in to help qualitatively select adequate member stocks to construct target portfolios.

In recent research examining market responses to corporate cyber incidents, significant insights for corporate strategy emerge. Directly involved corporations witness market reactions closely tied to their historical characteristics, like financial health and operational stability, emphasising the need for a robust corporate profile to counter potential cyber risks. Meanwhile, indirectly involved firms benefit from clear communication about their roles in incidents to prevent unwarranted reputational damage. The market's amplified reactions to novel cyber threats highlight the urgency of preparedness, especially for firms previously unexposed to major cyber incidents. Interestingly, market responses remain uniform regardless of an incident's severity, suggesting businesses should prioritise cyber resilience and transparent communication over the incident's magnitude. As cyber risks increasingly intertwine with corporate image and stakeholder trust, companies must transition from viewing them as mere technical challenges to strategic imperatives. This holistic approach, which stresses proactive steps, continuous adaptation, and consistent transparency, becomes vital for maintaining market trust and corporate resilience. Overall, this research underscores the multifaceted implications of cyber incidents on corporate financial health. The findings highlight the financial market's nuanced perceptions, demonstrating its ability to discern, amongst many factors, between primary and tangential actors while weighing corporate resilience. Notably, while the digital landscape continues to evolve, so does the importance of cybersecurity as an integral aspect of corporate strategy.

References

Abdelsalam, O., D. F. Ahelegbey, and Y. Essanaani (2023). The nexus of conventional, religious and ethical indices. *Available on SSRN*.

Akyildirim, E., S. Corbet, M. Efthymiou, C. Guiomard, J. O'Connell, and A. Sensoy (2020). The financial market effects of international aviation disasters. *International Review of Financial Analysis 69*.

Akyildirim, E., S. Corbet, A. Sensoy, and L. Yarovaya (2020). The impact of blockchain-related name changes on corporate performance. *Journal of Corporate Finance 65*, 101759.

Bollerslev, T. (1986). Generalized autoregressive conditional heteroskedasticity. *Journal of Econometrics 31*(3), 307–327.

Bouslah, K., J. Liñares-Zegarra, B. M'Zali, and B. Scholtens (2018). Ceo risk-taking incentives and socially irresponsible activities. *British Accounting Review 50*(1), 76–92.

Capelle-Blancard, G. and A. Petit (2019). Every little helps? esg news and stock market reaction. *Journal of Business Ethics 157*, 543–565.

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

Corbet, S., C. Larkin, B. Lucey, A. Meegan, and L. Yarovaya (2020). Cryptocurrency reaction to fomc announcements: Evidence of heterogeneity based on blockchain stack position. *Journal of Financial Stability 46*.

Crosignani, M., M. Macchiavelli, and A. F. Silva (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics 147*(2), 432–448.

Engle, R. F. (1982). Autoregressive conditional heteroscedasticity with estimates of the variance of united kingdom inflation. *Econometrica*, 987–1007.

Fiordelisi, F., M.-G. Soana, and P. Schwizer (2014). Reputational losses and operational risk in banking. *The European Journal of Finance 20*(2), 105–124.

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

Friedman, A. and S. Miles (2001). Socially responsible investment and corporate social and environmental reporting in the uk: An explaratory study. *British Accounting Review 33*(4), 523–548.

Gillet, R., G. Hübner, and S. Plunus (2010). Operational risk and reputation in the financial industry. *Journal of Banking & Finance 34*(1), 224–235.

Gualandris, J., A. Longoni, D. Luzzini, and M. Pagell (2021). The association between supply chain structure and transparency: A large-scale empirical study. *Journal of Operations Management 67*(7), 803 – 827.

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

Kumarasiri, J. and A. Gunasekarage (2017). Risk regulation, community pressure and the use of management accounting in managing climate change risk: Australian evidence. *British Accounting Review 49*(1), 25–38.

Li, J. and D. Wu (2020). Do corporate social responsibility engagements lead to real environmental, social, and governance impact? *Management Science 66*(6), 2564 – 2588.

Meegan, A., S. Corbet, C. Larkin, and B. Lucey (2021). Does cryptocurrency pricing response to regulatory intervention depend on underlying blockchain architecture? *Journal of International Financial Markets, Institutions and Money 70*.

Moll, J. and O. Yigitbasioglu (2019). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *British Accounting Review 51*(6).

Nelson, D. B. (1991). Conditional heteroskedasticity in asset returns: A new approach. *Econometrica*, 347–370.

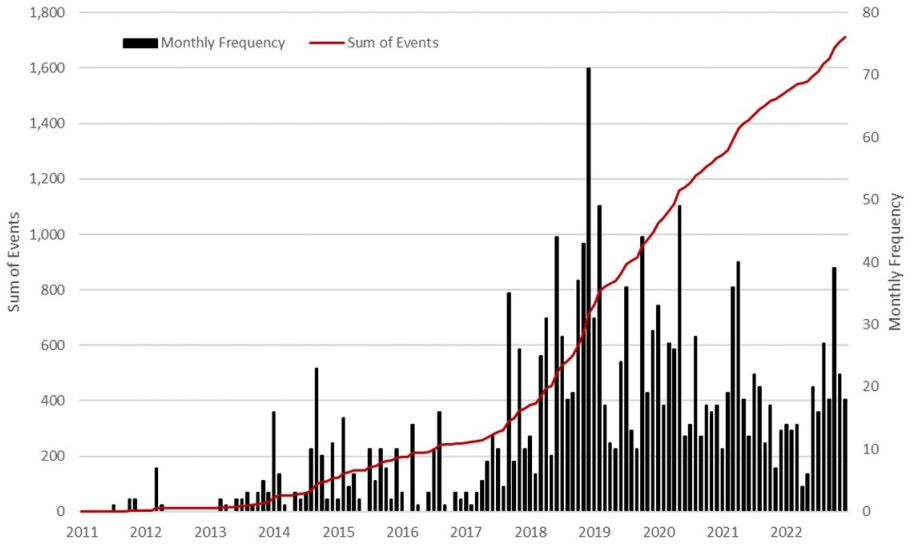
Schiemann, F. and R. Tietmeyer (2022). ESG controversies, ESG disclosure and analyst forecast accuracy. *International Review of Financial Analysis 84*.

Sturm, P. (2013). Operational and reputational risk in the european banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization 85*, 191–206.

Wang, S. L. and D. Li (2019). Responding to public disclosure of corporate social irresponsibility in host countries: Information control and ownership control. *Journal of International Business Studies 50*(8), 1283 – 1309.

Wong, J. B. and Q. Zhang (2022). Stock market reactions to adverse esg disclosure via media channels. *The British Accounting Review 54*(1), 101045.

Figure 1: Frequency of Cyberattacks and Privacy Violations (2011 through 2022)

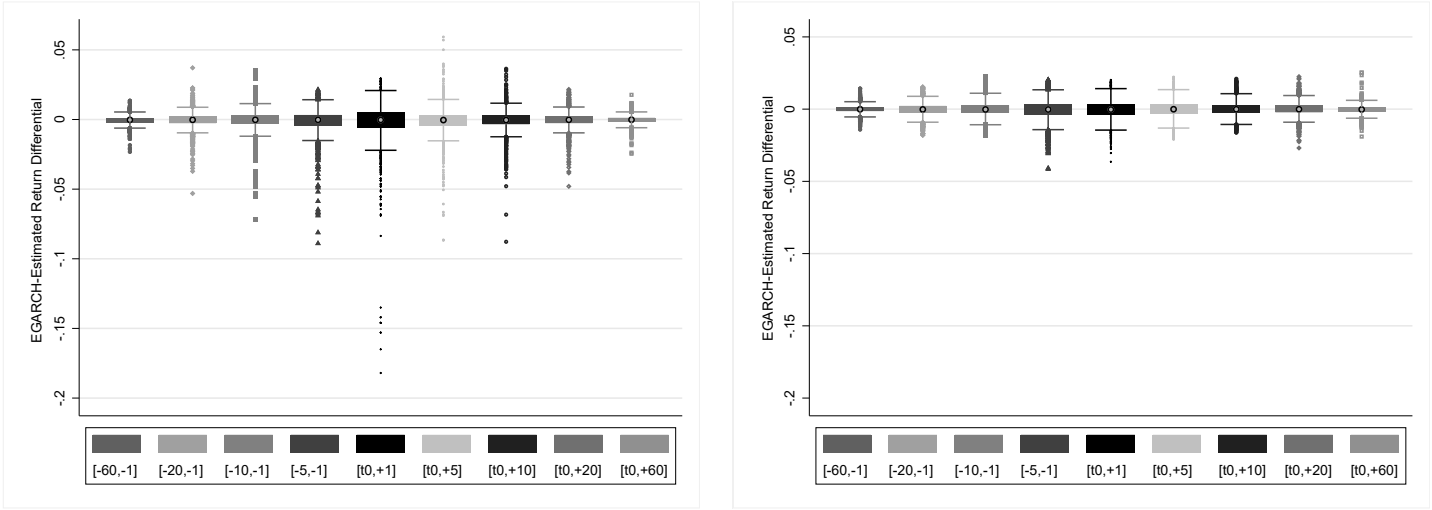


Note: The above Figure represents the cyberattack and privacy violation data collated from RepRisk, which has a structured framework of 28 core ESG issues that drive their research process. These issues are comprehensive and mutually exclusive, forming the foundation for linking and categorising risk incidents within their dataset. This framework helps ensure that every risk incident is associated with at least one of these 28 ESG issues. Specifically, a cyberattack is defined as a premeditated infiltration of computer systems, technology-based businesses, and networks. A cyberattack is a deliberate and premeditated attempt to breach the security of computer systems, technology-based businesses, and networks for various malicious purposes. These attacks can involve unauthorised access, theft, manipulation, or destruction of digital information and resources. Cyberattacks can target individuals, organisations, governments, and even critical infrastructure, with the intention of causing harm, extracting valuable data, disrupting operations, or gaining control over systems. Whereas a privacy violation is defined as actions by a company that result in the unauthorised access or distribution of an individual's personal information without his or her permission of knowledge. It commonly occurs through indirectly failing to protect privacy, i.e. outside data hacking and loss of client info, or directly violating privacy, i.e. phone/account hacking by a company or sale/release of confidential client info. Indeed, privacy violations refer to instances where an individual's personal information, data, or rights to privacy are compromised or infringed upon without their consent. These violations can occur in various contexts, such as online interactions, data breaches, surveillance, or unauthorised sharing of personal information. Privacy violations can have significant consequences for individuals, including loss of control over their personal data, potential identity theft, and erosion of their fundamental right to privacy.

Figure 2: EGARCH-estimated return differential due to cyberattack and privacy violations

i) Cyberattack and privacy violations

ii) Placebo testing sample (6-month)



Note: To identify the financial market response differentials to cyberattack and privacy violations, we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_4 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. In total, 77,220 EGARCH methodologies are analysed, considering nine windows of analysis surrounding the 1,716 analysed events and the multiple robustness testing procedures considered.

Table 1: Summary statistics relating to the corporations within the analysed samples separated by geographic region of headquarters

							Percentile							
	Mean	Var	Skew	Kurt	Min	Max	1%	5%	10%	25%	75%	90%	95%	99%
AU	0.0004	0.0001	-0.0974	11.72	-0.0970	0.0891	-0.0249	-0.0135	-0.0093	-0.0042	0.0052	0.0099	0.0142	0.0241
CH	0.0003	0.0001	-0.6003	10.01	-0.0816	0.0615	-0.0199	-0.0113	-0.0076	-0.0032	0.0041	0.0082	0.0112	0.0198
CN	0.0005	0.0002	-0.1503	4.11	-0.0669	0.1007	-0.0378	-0.0194	-0.0137	-0.0059	0.0074	0.0147	0.0196	0.0323
CY	-0.0004	0.0007	0.4296	14.20	-0.1976	0.2000	-0.0681	-0.0375	-0.0267	-0.0113	0.0100	0.0257	0.0382	0.0732
DE	0.0004	0.0002	-0.1929	8.17	-0.1422	0.1215	-0.0339	-0.0214	-0.0146	-0.0060	0.0071	0.0151	0.0200	0.0349
DK	0.0004	0.0002	-0.1443	5.07	-0.1136	0.0849	-0.0336	-0.0198	-0.0142	-0.0067	0.0074	0.0157	0.0212	0.0352
ES	0.0002	0.0002	-0.3404	10.36	-0.1340	0.1174	-0.0348	-0.0197	-0.0133	-0.0063	0.0069	0.0140	0.0193	0.0328
FI	0.0002	0.0002	-0.0974	5.63	-0.1272	0.1047	-0.0386	-0.0225	-0.0161	-0.0068	0.0079	0.0156	0.0219	0.0359
FR	0.0003	0.0002	-0.0951	5.64	-0.1006	0.0935	-0.0347	-0.0197	-0.0134	-0.0057	0.0068	0.0138	0.0189	0.0306
GB	0.0010	0.0002	-0.1760	4.82	-0.1212	0.1102	-0.0424	-0.0239	-0.0167	-0.0068	0.0093	0.0180	0.0251	0.0423
GR	0.0004	0.0006	0.1844	6.46	-0.1728	0.2090	-0.0700	-0.0372	-0.0266	-0.0117	0.0117	0.0277	0.0413	0.0725
HK	0.0005	0.0003	0.1380	8.84	-0.1689	0.1685	-0.0386	-0.0245	-0.0174	-0.0077	0.0085	0.0188	0.0252	0.0442
ID	0.0006	0.0002	0.3759	4.79	-0.0937	0.0839	-0.0336	-0.0177	-0.0122	-0.0051	0.0058	0.0137	0.0205	0.0401
IE	0.0007	0.0002	-0.1683	8.89	-0.1245	0.1165	-0.0361	-0.0201	-0.0130	-0.0049	0.0069	0.0139	0.0194	0.0368
IL	-0.0004	0.0005	0.6110	9.81	-0.2244	0.2167	-0.0621	-0.0333	-0.0238	-0.0098	0.0056	0.0222	0.0391	0.0715
IN	0.0008	0.0002	0.0637	8.82	-0.1388	0.1328	-0.0355	-0.0201	-0.0144	-0.0064	0.0080	0.0157	0.0221	0.0363
IS	0.0000	0.0010	-0.7199	55.83	-0.4872	0.5000	-0.0915	-0.0340	-0.0222	-0.0076	0.0076	0.0241	0.0370	0.0876
IT	0.0002	0.0003	-0.4957	7.38	-0.1733	0.1076	-0.0453	-0.0273	-0.0193	-0.0086	0.0095	0.0193	0.0272	0.0436
JP	0.0004	0.0001	-0.5174	7.50	-0.0935	0.0730	-0.0277	-0.0156	-0.0112	-0.0042	0.0056	0.0115	0.0151	0.0253
KR	0.0003	0.0001	-0.3885	8.89	-0.0997	0.0774	-0.0265	-0.0142	-0.0098	-0.0039	0.0050	0.0103	0.0139	0.0226
LU	0.0005	0.0001	0.4793	7.91	-0.0546	0.1160	-0.0338	-0.0171	-0.0107	-0.0018	0.0027	0.0129	0.0187	0.0343
MX	0.0006	0.0003	-0.4232	26.19	-0.2500	0.1655	-0.0404	-0.0222	-0.0157	-0.0064	0.0067	0.0176	0.0261	0.0470
MY	0.0001	0.0006	0.4249	5.31	-0.1370	0.1768	-0.0657	-0.0356	-0.0244	-0.0105	0.0100	0.0253	0.0389	0.0744
NL	0.0007	0.0002	-0.2279	5.82	-0.1368	0.0985	-0.0428	-0.0228	-0.0161	-0.0068	0.0086	0.0170	0.0242	0.0391
NO	0.0003	0.0001	9.5156	320.09	-0.0886	0.3626	-0.0246	-0.0141	-0.0100	-0.0047	0.0049	0.0108	0.0151	0.0245
NZ	0.0002	0.0003	-1.4959	29.78	-0.2377	0.1344	-0.0430	-0.0215	-0.0155	-0.0070	0.0079	0.0166	0.0225	0.0422
PH	0.0004	0.0002	0.7853	11.17	-0.1047	0.1372	-0.0339	-0.0199	-0.0141	-0.0064	0.0070	0.0152	0.0214	0.0392
PK	0.0007	0.0003	7.8276	212.24	-0.0898	0.4946	-0.0386	-0.0206	-0.0141	-0.0068	0.0076	0.0159	0.0225	0.0397
PT	0.0003	0.0002	-0.4014	5.09	-0.1384	0.0995	-0.0425	-0.0242	-0.0170	-0.0076	0.0088	0.0175	0.0242	0.0394
RU	0.0007	0.0004	-1.6368	33.51	-0.3646	0.1245	-0.0527	-0.0271	-0.0184	-0.0083	0.0098	0.0210	0.0307	0.0568
SA	0.0002	0.0001	0.2075	9.88	-0.0811	0.0959	-0.0335	-0.0168	-0.0106	-0.0034	0.0034	0.0118	0.0189	0.0335
SE	0.0001	0.0001	0.3631	7.46	-0.0943	0.1179	-0.0336	-0.0187	-0.0130	-0.0058	0.0059	0.0129	0.0190	0.0323
SG	0.0001	0.0001	0.2181	6.75	-0.0765	0.0821	-0.0258	-0.0146	-0.0106	-0.0047	0.0051	0.0107	0.0146	0.0266
TH	0.0002	0.0002	-0.1558	8.86	-0.1418	0.0995	-0.0368	-0.0197	-0.0145	-0.0063	0.0063	0.0146	0.0217	0.0406
TW	0.0004	0.0002	-0.3046	3.23	-0.0765	0.0725	-0.0363	-0.0197	-0.0138	-0.0064	0.0074	0.0146	0.0200	0.0328
US	0.0004	0.0003	-0.1151	17.99	-0.1755	0.1743	-0.0371	-0.0222	-0.0159	-0.0069	0.0076	0.0159	0.0228	0.0424

Note: To investigate the effects of cyberattack and privacy violation events upon corporate returns, we first proceed to match events identified from the RepRisk database with each identified ISIN code, where stock data is obtained for the period 1 January 2010 through 30 June 2023, where related summary statistics relating to each country analysed are presented in the Table above. Stock market data selection was considered within the context of providing a strong sample of data both before and after the events identified and collated through the RepRisk database. Therefore, extended stock market data is obtained to generate a strong sample period of analysis to adequately represent stock market behaviour both before and after the earliest and latest events recorded in our sample.

Table 2: Summary statistics relating to the EGARCH-estimated return differentials due to cyberattack and privacy violation incidents

					Percentile					
	Mean	Var	Skew	Kurt	1%	5%	10%	90%	95%	99%
					Primary Group					
(-60,-1)	-0.0005	0.0000	-0.8702	6.0771	-0.0096	-0.0060	-0.0039	0.0027	0.0040	0.0077
(-20,-1)	-0.0005	0.0000	-1.2867	12.1819	-0.0172	-0.0089	-0.0056	0.0046	0.0068	0.0131
(-10,-1)	-0.0006	0.0001	-1.6382	13.5830	-0.0227	-0.0118	-0.0073	0.0063	0.0099	0.0180
(-5,-1)	-0.0012	0.0001	-2.8149	18.0898	-0.0339	-0.0143	-0.0099	0.0077	0.0113	0.0165
(t_0,+1)	-0.0024	0.0003	-4.6709	37.4577	-0.0601	-0.0247	-0.0152	0.0109	0.0149	0.0270
(t_0,+5)	-0.0011	0.0001	-1.5769	14.6350	-0.0405	-0.0158	-0.0108	0.0082	0.0120	0.0255
(t_0,+10)	-0.0008	0.0001	-1.7660	16.1680	-0.0298	-0.0125	-0.0080	0.0062	0.0099	0.0190
(t_0,+20)	-0.0006	0.0000	-1.3667	9.2948	-0.0190	-0.0093	-0.0061	0.0047	0.0069	0.0146
(t_0,+60)	-0.0003	0.0000	-0.7589	7.1749	-0.0096	-0.0051	-0.0038	0.0028	0.0042	0.0076
					Placebo Group					
(-60,-1)	-0.0001	0.0000	-0.0236	1.7429	-0.0054	-0.0034	-0.0024	0.0020	0.0029	0.0051
(-20,-1)	-0.0001	0.0000	-0.1127	1.3246	-0.0084	-0.0049	-0.0033	0.0033	0.0046	0.0077
(-10,-1)	0.0001	0.0000	0.1699	0.9878	-0.0093	-0.0058	-0.0042	0.0043	0.0062	0.0106
(-5,-1)	0.0001	0.0000	-0.4509	1.7661	-0.0119	-0.0093	-0.0061	0.0051	0.0074	0.0118
(t_0,+1)	0.0001	0.0000	-0.1417	0.8734	-0.0102	-0.0089	-0.0061	0.0057	0.0080	0.0121
(t_0,+5)	0.0001	0.0000	0.0412	0.7249	-0.0113	-0.0074	-0.0050	0.0054	0.0077	0.0117
(t_0,+10)	0.0002	0.0000	0.2765	1.0187	-0.0088	-0.0057	-0.0041	0.0044	0.0064	0.0113
(t_0,+20)	0.0000	0.0000	-0.0923	2.1060	-0.0091	-0.0054	-0.0037	0.0035	0.0050	0.0090
(t_0,+60)	-0.0001	0.0000	0.5191	6.3085	-0.0057	-0.0032	-0.0023	0.0022	0.0030	0.0052

Note: The above Table presents the summary statistics of the respective EGARCH methodologies that were implemented to identify the financial market response differentials due to cyberattacks and privacy breaches; where we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. Alternative methodological specifications and windows of analyses were omitted for brevity of presentation but are available from the authors upon request. Placebo group tests correspond to those methodologies implemented upon dummy variables utilising windows that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach.

Table 3: Corporate return differentials as separated by event sharpness

	[-60,-1]	[-20,-1]	[-10,-1]	[-5,-1]	[t_0,+1]	[t_0,+5]	[t_0,+10]	[t_0,+20]	[t_0,+60]
					Primary Group				
Direct	-0.0015	-0.0002	-0.0003	-0.0011***	-0.0025***	-0.0011***	-0.0008***	-0.0006***	-0.0003**
	(0.0001)	(0.0001)	(0.0002)	(0.0002)	(0.0004)	(0.0003)	(0.0002)	(0.0001)	(0.0001)
Indirect	-0.0005	-0.0006	-0.0006***	-0.0016**	-0.0020*	-0.0012	-0.0009	-0.0007	-0.0007**
	(0.0004)	(0.0003)	(0.0001)	(0.0006)	(0.0009)	(0.0007)	(0.0005)	(0.0004)	(0.0002)
					Placebo Group				
Direct	-0.0001	-0.0001	0.0001	-0.0002	-0.0002	0.0002	0.0002	0.0000	-0.0001
	(0.0001)	(0.0001)	(0.0001)	(0.0002)	(0.0002)	(0.0002)	(0.0001)	(0.0001)	(0.0001)
Indirect	-0.0001	-0.0001	-0.0002	-0.0001	-0.0002	-0.0002	0.0000	-0.0002	-0.0002
	(0.0002)	(0.0004)	(0.0004)	(0.0006)	(0.0005)	(0.0005)	(0.0004)	(0.0003)	(0.0002)

Note: To identify the financial market response differentials due to cyberattacks and privacy breaches, we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. Alternative methodological specifications and windows of analyses were omitted for brevity of presentation but are available from the authors upon request. Placebo group tests correspond to those methodologies implemented upon dummy variables utilising windows that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 4: Corporate return differentials as separated by event severity

	[-60,-1]	[-20,-1]	[-10,-1]	[-5,-1]	[t_0,+1]	[t_0,+5]	[t_0,+10]	[t_0,+20]	[t_0,+60]
					Primary Group				
High Severity	-0.0002	-0.0005	-0.0006	-0.0011	-0.0032***	-0.0034***	-0.0022**	-0.0011	-0.0004
	(0.0003)	(0.0007)	(0.0008)	(0.0008)	(0.0009)	(0.0009)	(0.0007)	(0.0006)	(0.0004)
Low Severity	-0.0002	-0.0002	-0.0006**	-0.0012***	-0.0024***	-0.0010***	-0.0008***	-0.0006***	-0.0003***
	(0.0001)	(0.0001)	(0.0002)	(0.0002)	(0.0004)	(0.0003)	(0.0002)	(0.0001)	(0.0001)
					Placebo Group				
High Severity	-0.0001	-0.0001	0.0001	-0.0003	-0.0003	0.0001	0.0002	0.0000	-0.0001
	(0.0001)	(0.0001)	(0.0001)	(0.0002)	(0.0002)	(0.0002)	(0.0001)	(0.0001)	(0.0001)
Low Severity	0.0000	-0.0001	-0.0001	-0.0001	-0.001	0.0001	0.0001	0.0001	0.0001
	(0.0004)	(0.0005)	(0.0007)	(0.0010)	(0.0010)	(0.0009)	(0.0008)	(0.0006)	(0.0007)

Note: To identify the financial market response differentials due to cyberattacks and privacy breaches, we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. Alternative methodological specifications and windows of analyses were omitted for brevity of presentation but are available from the authors upon request. Placebo group tests correspond to those methodologies implemented upon dummy variables utilising windows that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 5: Corporate return differentials as separated by event reach

	[-60,-1]	[-20,-1]	[-10,-1]	[-5,-1]	[t_0,+1]	[t_0,+5]	[t_0,+10]	[t_0,+20]	[t_0,+60]
					Primary Group				
Broad Reaching	-0.0001	-0.0004	-0.0004	-0.0010**	-0.0022***	-0.0014***	-0.0014***	-0.0008***	-0.0005***
	(0.0001)	(0.0002)	(0.0003)	(0.0004)	(0.0006)	(0.0004)	(0.0003)	(0.0002)	(0.0001)
Narrow Reaching	-0.0002	-0.0004	-0.0005	-0.0009*	-0.0019***	-0.0001***	0.0001	-0.0004	-0.0002
	(0.0001)	(0.0002)	(0.0003)	(0.0004)	(0.0005)	(0.0004)	(0.0003)	(0.0002)	(0.0001)
					Placebo Group				
Broad Reaching	-0.0001	-0.0003	0.0001	-0.0003	-0.0001	-0.0003	0.0000	-0.0001	-0.0002
	(0.0001)	(0.0002)	(0.0002)	(0.0003)	(0.0003)	(0.0003)	(0.0002)	(0.0002)	(0.0001)
Narrow Reaching	-0.0003	-0.0001	0.0000	-0.0002	-0.0005	0.0001	0.0000	0.0000	-0.0001
	(0.0001)	(0.0002)	(0.0003)	(0.0003)	(0.0003)	(0.0003)	(0.0002)	(0.0002)	(0.0001)

Note: To identify the financial market response differentials due to cyberattacks and privacy breaches, we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. Alternative methodological specifications and windows of analyses were omitted for brevity of presentation but are available from the authors upon request. Placebo group tests correspond to those methodologies implemented upon dummy variables utilising windows that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 6: Corporate return differentials as separated by event novelty

	[-60,-1]	[-20,-1]	[-10,-1]	[-5,-1]	[t_0,+1]	[t_0,+5]	[t_0,+10]	[t_0,+20]	[t_0,+60]
					Primary Group				
New Issue	-0.0002	-0.0003	-0.0007*	-0.0009*	-0.0016**	-0.0008***	-0.0009*	-0.0009**	-0.0006***
	(0.0002)	(0.0003)	(0.0003)	(0.0004)	(0.0006)	(0.0003)	(0.0004)	(0.0003)	(0.0002)
Re-occurring Issue	-0.0001	-0.0002	-0.0006*	-0.0013***	-0.0029***	-0.0013***	-0.0008***	-0.0005**	-0.0002*
	(0.0001)	(0.0002)	(0.0002)	(0.0003)	(0.0005)	(0.0003)	(0.0002)	(0.0002)	(0.0001)
					Placebo Group				
New Issue	-0.0001	-0.0003	0.0003	-0.0004	-0.0002	0.0002	0.0001	-0.0002	-0.0001
	(0.0001)	(0.0002)	(0.0002)	(0.0003)	(0.0003)	(0.0003)	(0.0002)	(0.0002)	(0.0002)
Re-occurring Issue	-0.0001	-0.0001	0.0000	-0.0003	-0.0001	0.0001	0.0003	0.0001	-0.0001
	(0.0001)	(0.0001)	(0.0002)	(0.0002)	(0.0002)	(0.0002)	(0.0002)	(0.0001)	(0.0001)

Note: To identify the financial market response differentials due to cyberattacks and privacy breaches, we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. Alternative methodological specifications and windows of analyses were omitted for brevity of presentation but are available from the authors upon request. Placebo group tests correspond to those methodologies implemented upon dummy variables utilising windows that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 7: Corporate return differentials as separated by event year (main testing sample)

	[-60,-1]	[-20,-1]	[-10,-1]	[-5,-1]	[t_0,+1]	[t_0,+5]	[t_0,+10]	[t_0,+20]	[t_0,+60]
2011	-0.0006	-0.0010	-0.0007	-0.0002	-0.0060	-0.0001	0.0005	0.0004	0.0007
	(0.0015)	(0.0014)	(0.0023)	(0.0025)	(0.0158)	(0.0063)	(0.0031)	(0.0021)	(0.0017)
2012	-0.0003	-0.0003	-0.0002	-0.0009	-0.0014	-0.0033	-0.0020	0.0004	0.0002
	(0.0006)	(0.0006)	(0.0005)	(0.0007)	(0.0013)	(0.0029)	(0.0016)	(0.0005)	(0.0003)
2013	-0.0015	-0.0026	-0.0036	-0.0038	-0.0007	-0.0032	-0.0005	-0.0009	0.0001
	(0.0009)	(0.0012)	(0.0020)	(0.0022)	(0.0035)	(0.0025)	(0.0005)	(0.0007)	(0.0010)
2014	0.0003	0.0002	-0.0003	0.0001	-0.0007	0.0003	-0.0003	-0.0002	0.0001
	(0.0002)	(0.0004)	(0.0005)	(0.0006)	(0.0010)	(0.0007)	(0.0005)	(0.0004)	(0.0003)
2015	0.0004	0.0002	0.0004	-0.0002	-0.0016	-0.0003	-0.0001	-0.0004	-0.0001
	(0.0003)	(0.0005)	(0.0007)	(0.0008)	(0.0012)	(0.0009)	(0.0006)	(0.0005)	(0.0003)
2016	-0.0004	-0.0003	-0.0012	-0.0019*	-0.0020*	-0.0018*	-0.0018*	-0.0012	-0.0012***
	(0.0004)	(0.0005)	(0.0007)	(0.0008)	(0.0009)	(0.0007)	(0.0007)	(0.0006)	(0.0003)
2017	-0.0001	-0.0002	-0.0013	-0.0034**	-0.0055***	-0.0032***	-0.0011	-0.0006	-0.0001
	(0.0003)	(0.0006)	(0.0010)	(0.0014)	(0.0005)	(0.0005)	(0.0007)	(0.0004)	(0.0002)
2018	-0.0003	-0.0003	-0.0004	-0.0008*	-0.0033***	-0.0003	-0.0002	-0.0004	-0.0001
	(0.0001)	(0.0002)	(0.0003)	(0.0004)	(0.0004)	(0.0005)	(0.0004)	(0.0003)	(0.0002)
2019	-0.0002	0.0000	0.0001	-0.0005***	-0.0053***	-0.0008*	-0.0006*	-0.0004	-0.0003*
	(0.0002)	(0.0002)	(0.0003)	(0.0001)	(0.0001)	(0.0004)	(0.0003)	(0.0003)	(0.0001)
2020	-0.0001	-0.0001	-0.0009	-0.0018*	-0.0030***	-0.0003	-0.0007	-0.0005	-0.0011***
	(0.0003)	(0.0005)	(0.0007)	(0.0008)	(0.0010)	(0.0008)	(0.0007)	(0.0005)	(0.0003)
2021	-0.0003	-0.0002	-0.0006	-0.0019***	-0.0031***	-0.0012*	-0.0010*	-0.0004	-0.0003
	(0.0002)	(0.0003)	(0.0004)	(0.0005)	(0.0004)	(0.0006)	(0.0005)	(0.0003)	(0.0002)
2022	-0.0001	-0.0005	-0.0006	-0.0004	-0.0068***	-0.0033***	-0.0022***	-0.0020***	-0.0003
	(0.0002)	(0.0004)	(0.0005)	(0.0007)	(0.0019)	(0.0008)	(0.0006)	(0.0005)	(0.0002)

Note: To identify the financial market response differentials due to cyberattacks and privacy breaches, we utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur.***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 8: Corporate return differentials as separated by event year (Placebo group sample)

	[-60,-1]	[-20,-1]	[-10,-1]	[-5,-1]	[t_0,+1]	[t_0,+5]	[t_0,+10]	[t_0,+20]	[t_0,+60]
2011	-0.0011	-0.0034	-0.0003	0.0029	0.0045	0.0039	0.0032	0.0015	-0.0011
	(0.0012)	(0.0013)	(0.0005)	(0.0040)	(0.0044)	(0.0019)	(0.0019)	(0.0008)	(0.0007)
2012	-0.0004	-0.0011	-0.0004	0.0004	-0.0005	0.0002	0.0012	-0.0003	0.0001
	(0.0004)	(0.0009)	(0.0010)	(0.0009)	(0.0008)	(0.0011)	(0.0011)	(0.0007)	(0.0003)
2013	0.0001	-0.0010	-0.0008	0.0036	0.0015	0.0028	0.0015	-0.0006	0.0006
	(0.0007)	(0.0014)	(0.0015)	(0.0022)	(0.0023)	(0.0027)	(0.0019)	(0.0020)	(0.0007)
2014	0.0002	-0.0001	-0.0003	0.0000	-0.0006	0.0008	0.0007	0.0003	-0.0002
	(0.0002)	(0.0004)	(0.0005)	(0.0006)	(0.0007)	(0.0007)	(0.0004)	(0.0003)	(0.0002)
2015	-0.0005	0.0000	-0.0002	-0.0002	-0.0002	-0.0009	0.0002	-0.0001	-0.0007
	(0.0003)	(0.0005)	(0.0006)	(0.0009)	(0.0009)	(0.0007)	(0.0006)	(0.0005)	(0.0005)
2016	-0.0006	0.0002	-0.0009	-0.0016	-0.0017	-0.0007	-0.0002	-0.0002	0.0004
	(0.0004)	(0.0006)	(0.0010)	(0.0010)	(0.0013)	(0.0008)	(0.0007)	(0.0004)	(0.0003)
2017	0.0003	0.0004	0.0004	0.0006	0.0009	0.0007	0.0007	0.0003	0.0004
	(0.0002)	(0.0003)	(0.0005)	(0.0006)	(0.0006)	(0.0005)	(0.0005)	(0.0003)	(0.0002)
2018	0.0001	0.0001	0.0002	-0.0004	-0.0002	0.0005	0.0003	-0.0003	-0.0002
	(0.0001)	(0.0002)	(0.0003)	(0.0004)	(0.0004)	(0.0003)	(0.0003)	(0.0002)	(0.0002)
2019	-0.0003	-0.0004	-0.0005	-0.0002	-0.0005	0.0001	0.0001	-0.0002	-0.0003
	(0.0002)	(0.0003)	(0.0003)	(0.0005)	(0.0004)	(0.0004)	(0.0003)	(0.0003)	(0.0002)
2020	0.0002	0.0002	0.0003	-0.0007	-0.0004	0.0001	0.0001	0.0003	0.0004
	(0.0002)	(0.0003)	(0.0004)	(0.0005)	(0.0005)	(0.0005)	(0.0004)	(0.0003)	(0.0002)
2021	-0.0001	-0.0006	-0.0001	-0.0009	-0.0004	-0.0006	-0.0002	-0.0001	-0.0001
	(0.0002)	(0.0003)	(0.0004)	(0.0005)	(0.0005)	(0.0005)	(0.0004)	(0.0004)	(0.0002)
2022	0.0000	0.0001	0.0005	-0.0006	-0.0005	-0.0005	-0.0004	0.0001	0.0001
	(0.0002)	(0.0003)	(0.0004)	(0.0005)	(0.0006)	(0.0004)	(0.0004)	(0.0004)	(0.0002)

Note: In the above Table, results correspond to placebo tests implemented upon dummy variables utilising windows that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. We utilise the mean equation of the EGARCH(1,1) methodology $r_t = a_0 + b_1 r_{t-1} + b_2 r_{t-2} + b_3 I_t + b_3 d_t + \varepsilon_t$, where the term d_t represents a dummy variable that takes a value of unity during the analysed window surrounding each respective reputational event. To adequately and robustly assess the time period surrounding each event, we measure return differentials as a result of reputational disaster across multiple estimation windows of three months after each identified event across a variety of different event windows, including [-60,-1], [-20,-1], [-10,-1], [-5,-1], [t_0,+1], [t_0,+5], [t_0,+10], [t_0,+20], and [t_0,+60], to test the pricing response both before and after the dates on which significant reputational events are found to occur. Alternative methodological specifications and windows of analyses were omitted for brevity of presentation but are available from the authors upon request. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 9: Differential response to cyberattack and privacy violations based on respective corporate characteristics

	Cyberattack				Placebo Group			
	Model 1	Model 2	Model 3	Model 4	Model 1	Model 2	Model 3	Model 4
M.Cap	0.0026*	0.0026*	0.0026*	0.0065*	0.0012	0.0003	0.0003	0.0001
	(0.0007)	(0.0007)	(0.0007)	(0.0026)	(0.0016)	(0.0012)	(0.0012)	(0.0002)
Rev.Surprise		-0.0129***		-0.0111***		0.0039		0.0066
		(0.0007)		(0.0035)		(0.0033)		(0.0170)
Global Cred.Rank			-0.0019**	-0.0013*			-0.0013	-0.0020
			(0.0009)	(0.0007)			(0.0021)	(0.0020)
12m Vol.			-0.0007*	-0.0022*			-0.0009	0.0019
			(0.0004)	(0.0009)			(0.0008)	(0.0024)
Cred. Vol.			-0.0007*	-0.0022*			0.0018	0.0029
			(0.0004)	(0.0012)			(0.0009)	(0.0025)

Note: To provide additional explanatory value, the presented return differentials resulting from the RepRisk-defined cyberattack and privacy violations are then considered in a methodology that encapsulates a number of distinct corporate characteristics. Each selected variable has been considered for various reasons, primarily surrounding the many industrial and sectoral pressures that exist, to identify whether deteriorating financial performance can be observed as an explanatory factor when considering the financial market response to such significant breaches. The data considered include Revenue Surprise, the natural logarithm of company market capitalisation, the Credit Combined Global Rank, the twelve-month Volatility Rank, and the Credit Structural Asset Volatility Global Rank. We consider the results surrounding event windows $[t_0,+1]$ to test whether corporate characteristics can explain whether such differential stock market response diminishes or perhaps persists in varying manners due to corporate factors. All examined analysis windows were considered in this secondary analysis; however, for the brevity of presentation, only the event window $[t_0,+1]$ is presented. All other results are available from the authors upon request. Corresponding placebo group procedures represent dummy variables that utilise analyses windows based on dummy variables that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 10: Sharp-based differential response to cyberattack and privacy violations based on respective corporate characteristics

	Cyberattack				Placebo Group			
	Model 1	Model 2	Model 3	Model 4	Model 1	Model 2	Model 3	Model 4
				Sharp				
M.Cap	0.0022*	0.0022*	0.0022*	0.0015*	-0.0046	-0.0050	-0.0050	0.0076
	(0.0008)	(0.0008)	(0.0008)	(0.0006)	(0.0042)	(0.0043)	(0.0043)	(0.0204)
Rev.Surprise		-0.0030***		-0.0099***		0.0093		-0.0028
		(0.0008)		(0.0035)		(0.0281)		(0.0082)
GlobalCred.Rank			-0.0019**	-0.0015*			-0.0048	-0.0021
			(0.0009)	(0.0009)			(0.0051)	(0.0030)
12m Vol.			-0.0008*	-0.0021*			-0.0015	-0.0005
			(0.0005)	(0.0012)			(0.0013)	(0.0020)
Cred. Vol.			-0.0007*	-0.0021*			0.0023	-0.0005
			(0.0004)	(0.0012)			(0.0016)	(0.0021)
				Unsharp				
M.Cap	0.0129**	0.0111*	0.0111*	0.0152*	-0.0008	0.0053	0.0053	-0.0607
	(0.0064)	(0.0069)	(0.0069)	(0.0057)	(0.0054)	(0.0076)	(0.0076)	(0.0447)
Rev.Surprise		-0.0009		-0.0067		0.0015		0.0010
		(0.0033)		(0.0046)		(0.0020)		(0.0006)
Global Cred.Rank			-0.0014	-0.0007			-0.0048	-0.0036
			(0.0236)	(0.0031)			(0.0051)	(0.0045)
12m Vol.			-0.0024	-0.0061			-0.0015	0.0036
			(0.0048)	(0.0062)			(0.0013)	(0.0044)
Cred. Vol.			-0.0031	-0.0062			0.0023	0.0082
			(0.0070)	(0.0059)			(0.0016)	(0.0051)

Note: To provide additional explanatory value, the presented return differentials resulting from the RepRisk-defined cyberattack and privacy violations are then considered in a methodology that encapsulates a number of distinct corporate characteristics. Each selected variable has been considered for various reasons, primarily surrounding the many industrial and sectoral pressures that exist, to identify whether deteriorating financial performance can be observed as an explanatory factor when considering the financial market response to such significant breaches. The data considered include Revenue Surprise, the natural logarithm of company market capitalisation, the Credit Combined Global Rank, the twelve-month Volatility Rank, and the Credit Structural Asset Volatility Global Rank. We consider the results surrounding event windows $[t_0,+1]$ to test whether corporate characteristics can explain whether such differential stock market response diminishes or perhaps persists in varying manners due to corporate factors. All examined analysis windows were considered in this secondary analysis; however, for the brevity of presentation, only the event window $[t_0,+1]$ is presented. All other results are available from the authors upon request. Corresponding placebo group procedures represent dummy variables that utilise analyses windows based on dummy variables that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 11: Severity-based differential response to cyberattack and privacy violations based on respective corporate characteristics

	Cyberattack				Placebo Group			
	Model 1	Model 2	Model 3	Model 4	Model 1	Model 2	Model 3	Model 4
				High Severity				
M.Cap	0.0047**	0.0048**	0.0048**	0.0043**	0.0010	0.0002	0.0002	0.0371
	(0.0021)	(0.0022)	0.0022)	(0.0024)	(0.0034)	(0.0034)	(0.0034)	(0.0723)
Rev.Surprise		-0.0133***		-0.0196***		0.0034*		0.0520
		(0.0015)		(0.0012)		(0.0020)		(0.0313)
Global Cred.Rank			-0.0023**	-0.0026**			0.0005	0.0009
			(0.0008)	(0.0011)			(0.0018)	(0.0017)
12m Vol.			-0.0008	-0.006			-0.0023	-0.0059
			(0.0067)	(0.0479)			(0.0014)	(0.0078)
Cred. Vol.			-0.0098*	-0.0132**			0.0010	-0.0032
			(0.0053)	(0.0044)			(0.0010)	(0.0077)
				Low Severity				
M.Cap	0.0025***	0.0026***	0.0026***	0.0166***	0.0002	0.0001	0.0001	0.0292
	(0.0008)	(0.0008)	(0.0008)	(0.0013)	(0.0012)	(0.0012)	(0.0012)	(0.0253)
Rev.Surprise		-0.0149***		-0.0111***		0.0040		0.0192
		(0.0003)		(0.0035)		(0.0045)		(0.0132)
Global Cred.Rank			-0.0020**	-0.0013*			0.0000	-0.0008
			(0.0009)	(0.0007)			(0.0016)	(0.0015)
12m Vol.			-0.0007*	-0.0022*			-0.0001	-0.0026
			(0.0004)	(0.0013)			(0.0007)	(0.0025)
Cred. Vol.			-0.0008*	-0.0022*			0.0000	-0.0026
			(0.0004)	(0.0013)			(0.0007)	(0.0026)

Note: To provide additional explanatory value, the presented return differentials resulting from the RepRisk-defined cyberattack and privacy violations are then considered in a methodology that encapsulates a number of distinct corporate characteristics. Each selected variable has been considered for various reasons, primarily surrounding the many industrial and sectoral pressures that exist, to identify whether deteriorating financial performance can be observed as an explanatory factor when considering the financial market response to such significant breaches. The data considered include Revenue Surprise, the natural logarithm of company market capitalisation, the Credit Combined Global Rank, the twelve-month Volatility Rank, and the Credit Structural Asset Volatility Global Rank. We consider the results surrounding event windows $[t_0,+1]$ to test whether corporate characteristics can explain whether such differential stock market response diminishes or perhaps persists in varying manners due to corporate factors. All examined analysis windows were considered in this secondary analysis; however, for the brevity of presentation, only the event window $[t_0,+1]$ is presented. All other results are available from the authors upon request. Corresponding placebo group procedures represent dummy variables that utilise analyses windows based on dummy variables that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 12: Reach-based differential response to corporate characteristics

	Cyberattack				Placebo Group			
	Model 1	Model 2	Model 3	Model 4	Model 1	Model 2	Model 3	Model 4
				Wide Reach				
M.Cap	0.0044***	0.0046***	0.0046***	0.0047***	-0.0016	-0.0016	-0.0016	0.0221
	(0.0013)	(0.0013)	(0.0013)	(0.0018)	(0.0012)	(0.0012)	(0.0012)	(0.0284)
Rev.Surprise		-0.0057		-0.0114		-0.0024		-0.0135
		(0.0037)		(0.0070)		(0.0030)		(0.0104)
GlobalCred.Rank			-0.0027*	-0.0026*			-0.0018	-0.0022
			(0.0014)	(0.0014)			(0.0014)	(0.0014)
12m Vol.			-0.0011	-0.0015			0.0003	-0.0017
			(0.0008)	(0.0033)			(0.0008)	(0.0030)
Cred. Vol.			-0.0011*	-0.0016*			0.0002	-0.0019
			(0.0006)	(0.0006)			(0.0006)	(0.0030)
				Narrow Reach				
M.Cap	0.0047***	0.0045***	0.0047***	0.0047***	-0.0009	-0.0009	-0.0009	-0.0188
	(0.0013)	(0.0013)	(0.0013)	(0.0157)	(0.0014)	(0.0015)	(0.0015)	(0.0360)
Rev.Surprise		-0.0102*		-0.0094***		-0.0024		-0.0516
		(0.0048)		(0.0015)		(0.0090)		(0.0349)
GlobalCred.Rank			-0.0049**	-0.0029***			0.0025	-0.0056
			(0.0023)	(0.0006)			(0.0016)	(0.0041)
12m Vol.			-0.0007***	-0.0017***			-0.0006	0.0040
			(0.0001)	(0.002)			(0.0007)	(0.0035)
Cred. Vol.			-0.0021**	-0.0046***			-0.0009	0.0036
			(0.0010)	(0.0016)			(0.0006)	(0.0034)

Note: To provide additional explanatory value, the presented return differentials resulting from the RepRisk-defined cyberattack and privacy violations are then considered in a methodology that encapsulates a number of distinct corporate characteristics. Each selected variable has been considered for various reasons, primarily surrounding the many industrial and sectoral pressures that exist, to identify whether deteriorating financial performance can be observed as an explanatory factor when considering the financial market response to such significant breaches. The data considered include Revenue Surprise, the natural logarithm of company market capitalisation, the Credit Combined Global Rank, the twelve-month Volatility Rank, and the Credit Structural Asset Volatility Global Rank. We consider the results surrounding event windows $[t_0,+1]$ to test whether corporate characteristics can explain whether such differential stock market response diminishes or perhaps persists in varying manners due to corporate factors. All examined analysis windows were considered in this secondary analysis; however, for the brevity of presentation, only the event window $[t_0,+1]$ is presented. All other results are available from the authors upon request. Corresponding placebo group procedures represent dummy variables that utilise analyses windows based on dummy variables that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 13: Novelty-based differential response to corporate characteristics

	Cyberattack				Placebo Group			
	Model 1	Model 2	Model 3	Model 4	Model 1	Model 2	Model 3	Model 4
				High Novelty				
M.Cap	0.0052***	0.0054***	0.0054***	0.0041**	-0.0017	-0.0017	-0.0006	-0.0229
	(0.0016)	(0.0016)	(0.0016)	(0.0020)	(0.0015)	(0.0015)	(0.0021)	(0.0386)
Rev.Surprise		-0.0038		-0.0040		0.0000		0.0055
		(0.0039)		(0.0062)		(0.0029)		(0.0120)
Global Cred.Rank			-0.0031*	-0.0052***			-0.0002	0.0005
			(0.0017)	(0.0016)			(0.0010)	(0.0015)
12m Vol.			-0.0043***	-0.0033***			0.0013	0.0015
			(0.0009)	(0.0002)			(0.0038)	(0.0037)
Cred. Vol.			-0.0024***	-0.0053***			0.0015	0.0016
			(0.0008)	(0.0019)			(0.0035)	(0.0039)
				Low Novelty				
M.Cap	0.0013*	0.0014*	0.0014*	0.0024*	-0.0011	-0.0010	-0.0010	-0.0046
	(0.0008)	(0.0008)	(0.0008)	(0.0014)	(0.0008)	(0.0008)	(0.0008)	(0.0140)
Rev.Surprise		-0.0119***		-0.0129*		-0.0061		0.0158
		(0.0004)		(0.0071)		(0.0049)		(0.0262)
Global Cred.Rank			-0.0028***	-0.0023**			0.0025	-0.0009
			(0.0004)	(0.0012)			(0.0031)	(0.0009)
12m Vol.			-0.0010**	-0.0022*			0.0000	-0.0006
			(0.0004)	(0.0012)			(0.0004)	(0.0015)
Cred. Vol.			-0.0017***	-0.0017***			0.0006	0.0003
			(0.0004)	(0.0002)			(0.0005)	(0.0015)

Note: To provide additional explanatory value, the presented return differentials resulting from the RepRisk-defined cyberattack and privacy violations are then considered in a methodology that encapsulates a number of distinct corporate characteristics. Each selected variable has been considered for various reasons, primarily surrounding the many industrial and sectoral pressures that exist, to identify whether deteriorating financial performance can be observed as an explanatory factor when considering the financial market response to such significant breaches. The data considered include Revenue Surprise, the natural logarithm of company market capitalisation, the Credit Combined Global Rank, the twelve-month Volatility Rank, and the Credit Structural Asset Volatility Global Rank. We consider the results surrounding event windows $[t_0,+1]$ to test whether corporate characteristics can explain whether such differential stock market response diminishes or perhaps persists in varying manners due to corporate factors. All examined analysis windows were considered in this secondary analysis; however, for the brevity of presentation, only the event window $[t_0,+1]$ is presented. All other results are available from the authors upon request. Corresponding placebo group procedures represent dummy variables that utilise analyses windows based on dummy variables that are re-considered when progressed six months into the future from the original identified date of a cyberattack or privacy breach. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.