Cyber-attacks and Their Impact on The Financial Markets: An Empirical Analysis

Rajesh Kumar Tharumar

A Thesis

In

The John Molson School of Business

Presented in Partial Fulfillment of the Requirements

for the Degree of Master of Science (Finance) at

Concordia University

Montreal, Quebec, Canada

April 2024

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Rajesh Kumar Tharumar

Entitled: Cyber-attacks and their impact on the financial markets: An empirical analysis

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Finance)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair
Dr. Ravi Mateti

_____ Examiner
Dr. Frederick Davis

_____ Thesis Supervisor
Dr. Thomas Walker

Approved by _____
Dr. Frederick Davis, Interim Graduate Program Director

April 2024 _____
Dr. Anne-Marie Croteau, Dean John Molson School of Business

Abstract

Cyber-attacks and Their Impact on The Financial Markets: An Empirical Analysis

Rajesh Kumar Tharumar

Cyber-attacks are a global concern, escalating in frequency. Our study explores whether and how cyber-attacks affect the financial performance of the targeted firms. Unlike previous research, we examine not only attack incidence but also the financial consequences, considering attack and firm characteristics. In addition, our study is the first to explore whether the time frame over which an attack affects a targeted firm varies depending on the type of attack. While the former is reasonably well documented, the latter is not. Market responses are diverse and sometimes delayed, influenced by breach disclosure laws. Our study further examines whether market responses differ when the affected entity is a parent or a subsidiary. Our results suggest that — because each cyber-attack has its own distinct characteristics — an aggregation of instances produces diminished or no results because markets respond within different time frames and in different directions. Our findings disentangle these effects and thus make an important contribution: contrary to the often insignificant findings presented by prior studies, we find that cyber-attacks have, on average, severe financial repercussions for the target firms. Parent firms appear more adept at handling these repercussions and may benefit from their size and diversification, allowing them to mitigate negative stock price effects, while subsidiary firms are hit harder. Finally, we estimate the probability of a cybersecurity incident: we report a convex relationship between a firm's asset size and its susceptibility to (successful) cyber-attacks and a concave relationship between a firm's net income and its cybersecurity risk.

Keywords: Cyber-attack, Data breach, Risk management

Acknowledgments

I am profoundly grateful to my esteemed supervisor, Dr. Walker, whose guidance was instrumental in the completion of my thesis. His invaluable advice and unwavering support have been a beacon during my academic journey. The privilege of being his student has enriched my learning experience immeasurably. I extend my thanks to Victoria Kelly and Simone Donders for their invaluable help in fine-tuning and proofreading my thesis, ensuring its clarity and coherence. I am also grateful to the committee members, Prof. Ravi Mateti and Prof. Fredrick Davis, for their invaluable advice and guidance, which have significantly enriched the content and depth of my research.

Additionally, my sincere appreciation extends to Professor Dr. Dieter Gramlich of Baden-Württemberg Cooperative State University Heidenheim, and Postdoctoral Research Fellow Dr. Moein Karami of John Molson School of Business, Concordia University. Their generous support during my research activities at the John Molson School of Business has been a cornerstone of my academic growth. Their kindness will forever resonate with me. Special thanks once again to Dr. Thomas Walker for extending the invitation to regular meetings with his colleagues and PhD students, which provided a sense of belonging during my academic journey. I am grateful to the members of the group - Dr. Thomas Walker, Dr. Moein Karami, Dr. Fredrick Davis, Dr. Raad Jassim, Dr. Jane McGaughey, Dr. Hamed Khadivar, Christopher Duquet, Dr. Erkan Yonder and everyone else - for their camaraderie and warmth, making me feel welcome and supported.

Finally, my deepest gratitude is reserved for my family - my parents and my sister. Their unwavering love and support have been my stronghold in times of need. Their belief in me has been the wind beneath my wings, propelling me towards my goals. Thank you for being my constant source of inspiration and strength.

Table of Contents

List of Tables

List of Figures

I. Introduction

In today's hyper-connected digital world, the proliferation of digital technologies and the unprecedented reach of the internet have ushered in an age of convenience, efficiency, and innovation. However, these developments also expose users and providers to cyber-security threats, the risks of which are considered one of the current leading global concerns (World Economic Forum, 2023).[1] Cyber-security breaches can result in financial losses, the disruption of operations, and increasing market volatility, as well as damage to an entity's reputation. Although the financial loss from cyber-security breaches is difficult to quantify, a report from IBM (2023) estimates the global average cost of a data breach at USD 4.45 million, an inflation-adjusted increase of 23% since 2017.[2] Furthermore, the per-record cost of a data breach is USD 165, a 17% inflation-adjusted increase since 2017. The report also states that, for the 13th consecutive time, the United States of America (U.S.) ranks first for bearing the highest financial cost globally.

Multiple regulatory frameworks have been established by both the federal and state governments in the U.S. These include, for instance, the National Institute of Standards and Technology (NIST) cyber-security framework, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), and the Data Breach Notification Laws, to name but some. The Data Breach Notification Laws were enacted at the state level over the course of several years, starting with California in 2003. These laws are of particular interest to this study

[1] Each year, the World Economic Forum publishes the Global Risk Report based on a broad-ranging survey of investment professionals' risk perceptions. The reports explore the most severe risks that affect the global landscape over three different time frames: 1) current, 2) short term (2 years or less), and 3) long term (greater than 2 years but less than 10 years).

[2] The report published in 2023 is the 18th annual edition and is based on an independent study by the Ponemon Institute. Their report is based on data breaches in 553 organisations globally between March 2022 and March 2023.

because they govern organizational requirements to notify affected individuals and the authorities in the event of a data breach. The laws state that organisations must notify implicated parties "without unreasonable delay," however, on average, the time frame for notification ranges between 30 and 45 days with provisions for exceptions and extensions.

The data used in this study is primarily derived from notifications to the State Attorney Generals' Offices as stipulated by the states' breach notification laws. With this data, we try to discern the primary firm and breach characteristics that affect a firm's stock price reaction to a breach. We further examine the factors that drive a firm's susceptibility of being targeted in a cyber-attack. Our study is one of few to examine the timing of investor responses to a cyber-security breach by segregating our analysis into three time periods: 1) at the breach announcement, 2) after the breach but before the breach announcement, and 3) post–breach announcement. Within the scope of this study, we use cyber-security breaches and data breaches interchangeably.

The remainder of this paper is structured as follows: Section II provides a review of the existing literature. In Sections III and IV, we describe and perform a preliminary analysis of our sample. In Sections V and VI, we outline our methodology and discuss the results of our analysis. In Section VII, we draw conclusions based on our results.

II. Literature Review and Hypothesis Development

The efficient market hypothesis is one of the most researched topics in finance. The origins of the hypothesis can be traced to Eugene Fama's seminal work (Fama, 1970). The approach has now become a standard to analyse stock market reactions to any event, adverse or otherwise. In

our context, Fama's methodology has been by employed by Corbet and Gurdgiev, (2019) to analyse the market reaction to cyber-attacks. The authors consider 518 data breaches in the period 2005-2015 and conclude that cyber-attacks are associated with an unexpected negative shock to a firms' reputation. This observation has been further attested to by Berkman et al. (2018), Kamiya et al. (2018, 2021), and Tosun (2021). Kamiya et al. (2021) report that the abnormal stock price loss is more pronounced when the breach affects a firm's sales growth, but that the impact is reduced if the board is more vigilant. Considering the impacts on a firm's reputation, Lending et al. (2018) report that firms with smaller and more experienced boards are less likely to become the victims of a data breach. In addition, they report that following a data breach there is an increased probability of the CEO and CTO being fired and an increased emphasis by the affected firm on their corporate governance and social responsibility. Ettredge et al. (2018) report a higher probability of breaches in smaller and younger firms with trade secrets.

Florackis et al. (2023) build an index to predict the vulnerability of a firm to a cyber-attack. In their paper, they also examine the propagation of the impact down the supply chain by using the cyber-attack at Solar Winds as a case study. Similarly, Crosignani et al. (2023) look at the propagation of impacts and observe a permanent change in the supply chain that causes parties to terminate contracts. Westland (2020) models the probability of a cyber-attack on a firm based on disclosure requirements present in the Sarbanes-Oxley Act. Finally, Romanosky et al. (2011) studies the effectiveness of the regulatory landscape and reports that data breach disclosure laws have reduced identity theft by 6.1%. Finally, Biener et al. (2015) and Mukhopadhyay et al. (2013) examine the costs and benefits of cyber-security insurance. However, they are unable to identify

sufficient reasons to acquire cyber-risk insurance products. Similalrly, Eling and Loperfido (2017) examine data breaches in order to enhance risk measurement and insurance pricing. They conclude that two or more types of data breaches cannot be combined and doing so will only lead to erroneous pricing.

Our study on the financial loss from a data breach is similar to Aldasoro et al. (2022), Eling and Jung (2022), Eling and Wirfs (2019), and Welburn and Strong (2022). These studies examine the severity of a cyberattack based on firm size, contagion risk, and location. In contrast, Cummins et al. (2006), Gatzert and Schubert (2022), and Heidinger and Gatzert (2018) focus their analyses on the banking and insurance sector. We contribute to the growing literature by testing the following hypotheses:

Hypothesis 1: There is a significant abnormal stock price drop around the announcement of a cyber security incident.

Hypothesis 2: This stock price drop varies based on the type of breach and the industry in which the firm operates.

Hypothesis 3: Firms that exhibit characteristics that should make them more resilient to cyber-attacks (e.g., large, profitable firms and parent companies) or less appealing to attackers (e.g., small, unprofitable firms) experience less severe stock price declines following cyber incidents compared to companies lacking these attributes.

In our analysis, we examine several critical firm characteristics—industry sectors, parent vs. subsidiary status, size, and profitability—to discern their impact on market reactions to cyber incidents. These characteristics play a pivotal role in shaping a company's resilience to cyber

threats and its subsequent market perception following a breach. Industry sectors offer insights into the varying degrees of susceptibility to cyber threats across different sectors, aiding in the identification of specific vulnerabilities and risk management strategies tailored to each industry's needs. Additionally, distinguishing between parent and subsidiary companies provides valuable insights into the influence of corporate structure and governance mechanisms on vulnerability and market response. Company size serves as a proxy for resources and capabilities, helping to elucidate the relationship between organizational scale and resilience to cyber incidents. Furthermore, profitability is a key determinant of financial health and may impact a company's ability to mitigate cyber risks effectively. By examining these firm characteristics, we aim to deepen our understanding of the complex interplay between cybersecurity, firm dynamics, and financial market reactions surrounding a cyber-attack announcement, thereby informing more robust risk management strategies and enhancing market resilience in the face of cyber threats.

III. Data

We collect data on data breaches as published by the Privacy Rights Clearinghouse (PRC).[3] The PRC reports 9,016 incidents in the period 2005-2019, providing a detailed account of each event. The details include the type of the organisation, nature of the breach, number of records lost, etc. We filter the dataset and only retain publicly traded firms as well as private firms whose majority shareholder is a publicly traded firm. Afterward, we cross-verify the data and consolidate

[3] Privacy Rights Clearinghouse (https://privacyrights.org) is an active American non-profit organisation founded in 1992. The organisation intends help people with their rights and choices. The organisation focuses on increasing access to information, policy discussion, and data privacy. PRC is one of the earliest organisations to focus on privacy rights and issues. The organization compiles cybersecurity incidents from data breach notifications published under state data breach notification laws by the U.S. Department of Health and Human Services and various state Attorneys General.

duplicates or events affecting multiple subsidiaries of a single firm. Finally, we filter out event periods that are less than 30 days apart, to avoid biases resulting from overlapping.

*** Insert Figure 1 ***

Figure 1 demonstrates how these filtering criteria narrow our sample size to 891. For the remaining firms in our dataset the stock price returns are aggregated from the Centre for Research in Security Prices (CRSP), the financial information is aggregated from S&P's Compustat, and the breach sentiment data of the incident and the firms are from Google Trends. We use the CRSP value weighted index to proxy for market returns.

*** Insert Table 1 ***

Table 1 provides summary statistics for our sample. As shown in Table 1, our dataset includes information on 891 data breaches involving publicly traded U.S. corporations between January 1, 2005, and February 28, 2019.

IV. Variable Definition and Preliminary Analysis

Firm and Breach Characteristics

For each data breach occurrence leading to a loss of electronic data, PRC reports a variety of variables including the name of the organisation, date and location of the breach, number of records lost or affected, and the type of breach. To evaluate the impact of the breach, the number of records lost is scaled by a factor of 1,000,000. We also create a dummy variable to capture the severity of the breach when the number of records lost exceeds 10 million records. Table 2 provides detailed information on the variables used and their description.

*** Insert Table 2 ***

To provide some insights into whether market reactions vary across different sectors, we create dummy variables for each of the major industry groups. Further, we create a variety of dummy variables to capture the characteristics of the breach. The dummy variables measure 1) whether an event affects multiple entities, 2) whether an event directly affects the ultimate parent, 3) the different types of breaches, and 4) interaction terms between the parent dummy & sectors and the parent dummy & breach types.

To proxy for the public sentiment regarding the firm and cyber-security related concerns , we use data from Google trends. Specifically, we build indices using differential search trends on Google between the start and end of the week leading to the data breach, namely: 1) cybersecurity, 2) cyber crime, 3) data breach, and 4) the firm name. Finally, we include year controls to account for annual variations in the data breach.

Correlation Analysis

*** Insert Table 3 ***

Table 3 provides the results of a correlation analysis of all pairwise combination of our independent variables. All correlation coefficients in Table 3 are small in absolute magnitude and few are statistically insignificant. As such, they do not require any follow-up in our subsequent regression analysis.

V. Methodology

We use event study methodology to measure the abnormal stock returns of firms following a data breach incident. Event study methodology is derived from the efficient market hypothesis (Fama, 1970). The efficient market hypothesis states that stocks prices reflect all public

information of a firm's activities, and that any new material public information should alter the price rapidly, reflecting the revised investor sentiment of the firm performance. An event study measures the abnormal return as the difference between actual return and the expected return around the time of the event.

$$AR_{i,t} = R_{i,t} - E(R_{i,t}) \quad (1)$$

where $AR_{i,t}$ is the abnormal return of stock *i* on day *t*, $R_{i,t}$ is the actual return of the stock and $E(R_{i,t})$ is the expected return.

In this paper, we perform a short term event study to examine the impact of a data breach on a firm's stock price. Following the seminal work of MacKinlay (1997), we use a market model approach to estimate the expected return:

$$E(R_{i,t}) = \alpha + \beta R_{m,t} + \varepsilon_{i,t} \quad (2)$$

where $R_{i,t}$ is the return of stock *i* on day *t*, $R_{m,t}$ is the return of the market on day *t*, $\varepsilon_{i,t}$ is the error term, and α and β are the parameter estimates.

Among the plethora of market indices available, we chose the CRSP value weighted index as the reference market index. We employ an estimation period to calculate the expected return cover the period from *t* = -300 days to *t* = -46 days relative to the event day. In instances in which a firm has multiple data breaches in a 30-day period, we remove the later events from our analysis. Adding the abnormal returns over a given period yields the cumulative abnormal returns:

$$CAR_{i,T} = \sum AR_{i,t} \quad (3)$$

Next, we perform a univariate analysis and compare the impact of data breaches based on the nature of the breach and industry sectors using non-parametric mean and median tests. We classify our sample firms into quintiles based on the firm's asset size and compare the smallest and largest quintile.

Finally, to evaluate the cross-sectional determinants of the stock market reaction to data breaches, we explore how the abnormal returns across several pre-event, post-event, and event windows relate to various breach characteristics, firm characteristics, and investor sentiment.

$$Y_i = \alpha_0 + \sum_{j=1}^{n} \beta_{i,j} X_{i,j} + \sum_{k=1}^{m} \beta_{i,k} Z_{i,k} + \varepsilon_i \quad (4)$$

where, Y_i is the CAR of firm due to cyber-security incident *i* during period *t*, $X_{i,j}$ are n independent variables, $Z_{i,k}$ are the control variables, α and β are the regression coefficients, and ε_i is the error term.

VI. Results and Discussion

We start our empirical analysis by examining the cumulative average abnormal returns (CARs) over various time frames before, during, and after a data breach announcement. To account for the anticipation and the delayed effects, we compute CARs over several days to compare the market reaction prior to the event, during the event, and after the event.

*** Insert Table 4 ***

In Table 4, we tabulate the CARs over various time frames during and around the announcement of a data breach or cyber-security incident. Panel A of Table 4 reports varying levels of significance in test windows around the breach announcement. The strongest

significance is observed in the window (-1,+1). The parametric and non-parametric test, both indicate 1% significance. The mean and median CAR during the window is -22 basis points (bps) and -9 bps, respectively. Other timeframes in the event's proximity have mean CARs ranging between -10 and -20 bps and 5% to 10% statistical significance. However, the significance in the non-parametric test is lost in these timeframes. These results are similar to the results reported by Florackis et al. (2023) and Tosun (2021).

Panel B of Table 4 reports the CARs and associated significance tests for several event windows after the breach but before the breach announcement. The parametric test in the test window (-2, -1) has a weak significance at the 10% level. Furthermore, there is no sign of anticipation observed in the period preceding the cyberattack. Panel C of Table 4 reports the results for several test windows post breach announcement. The test windows exhibit statistical significance in the non-parametric test between 5% to 10%, and the median CARs range between 5 and 8 bps. The positive CARs can be indicative of remedial steps taken by the firms and the positive market reactions to these actions. Weak significance of the CARs in the days t-1, t+1, and t+2 are contrary to the results reported by Tosun (2021).

Panel D of Table 4 reports the CARs and the significance tests for a series of other timeframes. The results are in line with our primary observations: negative returns following the breach but before its announcement and positive returns in the days after the announcement, with statistical significance in some but not all windows.

*** Insert Figure 2 ***

Figure 2 plots the CARs over a (-10,+10) window for each type data breach. Theft of devices has a strong negative cumulative abnormal return, however the impact from theft of stationary devices is almost 10 times higher than the impact from theft of portable devices. The impact from stolen card information (debit, credit, and other banking transaction cards) causes the third highest losses. We further observe that the highest impact due to unintended disclosure is at *t-1* relative to the announcement date. This is to be expected, since the public announcement comes post the unintended disclosure by the firm. Although the impact is not as steep, the breach has a similar effect as an intentional data leak by an insider. This apparent difference can be attributed to the possibility of corrective measures employed in the case of a data leak by an insider. It is also noteworthy that cybersecurity incidents involving hacking attacks do not yield large negative cumulative abnormal returns. This phenomenon is most likely due to the aggregation of all the different third-party disruptions to a firm's network into a single variable.

Univariate Analysis

To better evaluate the impact of different breach types and the influence of firm characteristics on the returns following a cyber-security incident, we perform a series of univariate tests in which we test for differences in mean and median CARs after grouping our sample along different dimensions. The median tests are robust to outliers, while the mean tests are not. Hence, we winsorize the data on both tails at the 99% level. The univariate analysis provides some intuition heading into the regression analysis. We use two sample t-tests to test for the significance of differences in means and Kruskal-Wallis median test for the significance in the median difference. We construct subsamples based on the different firm and breach characteristics. The results are tabulated in Table 5.

*** Insert Table 5 ***

Panel A of table 5 tabulates and tests the difference in means and medians for firms in the first and fifth quintile of the firms' asset size across the test windows (0,0) and (-2,-1). The quintiles exhibit no significant differences in both the mean and median tests across any on the test windows. Panels B to I tabulate and test the differences in means and medians for each of the sectors, and Panels J to N tabulate and test the difference in means and medians based on the nature of the breach.

In the sectoral groupings, we observe that for firms in the financial sector (Panel B of Table 5) none of the test windows yield any significant results in the mean or the median tests. Firms in the Finance sector constitute the majority of the sample with 354 cyber-security events. This could signal better preparedness and anticipatory measures taken by the firms in an event of a cyber-security breach. Similar results are reported by Ettredge et al. (2018) and Kamiya et al. (2021) for the firms in this sector. Firms in the Construction sector (Panel C), the Manufacturing sector (Panel D) and the Transportation sector (Panel E), yield no significance in the mean or the median difference tests. The construction sector has the lowest representation in the sample with 4 firms, thus sample size itself may affect the power of the event study. As opposed to the lack of support for the returns in the transportation sector, Kamiya et al. (2021) report negative returns for the firms of this sector implying the need for further analysis to support the apparent difference.

The wholesale trade sector (Panel F), despite being the second least represented sector, exhibits strongly (1%) significant differences in the mean and median for the test windows (-1,-

2). The mean and median CARs for this sector are negative and lower than the mean and median CARs of all the remaining firms by approximately 180 bps in the test window (-2,-1). In the test window (0,0), the mean and the median difference tests are insignificant. Given the sample size, this can represent either the sector's recovery after the breach or the lack of power in the test due to the small sample size. The retail trade sector (Panel G) has weak significance (10% statistical significance) in the mean difference test in the test window (-2,-1). The impact on CARs is not as pronounced as compared to the wholesale trade sector. Kamiya et al. (2021) provide adequate support for the results observed for the firms in the wholesale trade and the retail trade sector. We postulate that these firms are much more reliant on the digital infrastructure to compete and track order fulfilment and the associated billing. Hence the negative returns in the test window prior to the announcement can be attributed to the discovery of the cyber-security incident before an announcement by the firm itself. Finally, contrary to the results of Kamiya et al. (2021) the service sector (Panel H), yield no significant results and the firms in the utility sector (Panel I) exhibit positive returns in the test window (0,0), despite the significance in the median difference test.

In the groupings based on the nature of the breach, the impact of breach due theft of card information (Panel J) and data breach due to theft of stationary devices (Panel M), we have 10% significance in the median test of the (0,0) event window. Despite the dissimilarity in the breach types both these breach types have CARs which are ~50 bps lower than the other breach types. It's conceivable that the records compromised in these breaches are easier for perpetrators to organize and subsequently monetize, as these records have higher degree of similarity and veracity.

The hacked breach type (Panel L) represents all disruption of the firm's network by an outside party. For instance, malware infection, successful phishing campaigns, ransomware threats, DDoS attack etc. Despite the weak (10%) significance in the median test of the event window (-2,-1) the median CAR for the breach type is higher than the other breach types. Despite being the largest breach type in the sample, the lack of a strong impact could be due to the aggregation of all the different third-party disruptions in the firm's network. The impact of a phishing campaign and that of a ransomware attack could have widely different repercussions to the firm's operations. Corbet and Gurdgiev (2019) report lack of support for hacking when the variable is very broadly defined.

Overall, the univariate analysis dissects and effectively differentiates the impact of cyber-attacks on the major industry grouping, however the test lacks the power to decern the impacts due different types of cyber-attacks. Eling and Loperfido (2017) argue the need to differentiate the various cyber-attacks to accurately measure and quantify the risk. Hence, we use multiple regression model specifications to further examine the investor reactions to the various breach type.

Regression Analysis

Although we uncover some interesting results in our univariate analysis, it does not consider the impact of changes in the other variables. Univariate tests for differences in the CARs between the largest and smallest firms in our sample did not yield any significance, however we hypothesize that asset size should play a significant role since it is indicative of a firm's ability to invest in counter or remedial measures (Ettredge et al. 2018). To examine this issue further, we include the second degree term (the square of Log (Total Assets)) in our subsequent analysis.

Regression Analysis – Base Model

In each window we regress the dependent variable (CAR) on the parameters, with year fixed effects to account for year specific variations. These may include annual improvements in technology that facilitate data breach such as skimming devices, software codes, etc.

*** Insert Table 6 ***

In Table 6, we tabulate the results of our analysis for three different groups: 1) the announcement window – test windows including the breach announcement date [(-1,+1) & (0,0)], 2) the pre-announcement window – test windows preceding the breach announcement date [(-1,-1) & (-2,-1)], and 3) the post-announcement window – test windows after the announcement date [(+1,+1) & (+1,+2)]. The sentiment proxies have varying levels of significance across the different event windows. The sign of the proxies cannot be used to interpret the direction of impact, because the proxies are estimated as the difference in the number of searches (scaled by the maximum number of searches in the year) at the end of the week compared to the start of the week. Hence, the peak of the searches can be at the start or end of the week. The cybercrime search trend is significant at the 1% level in the pre-announcement window (-1,-1). The cybersecurity search trend is insignificance in all test windows. The data breach search trend is significant at the 10% level in the post-announcement window (+1,+1). The firm search trend exhibits significance at the 10% level in the announcement window (-1,+1). Florackis et al. (2023) and Tosun (2021) have documented the effectiveness of using the data from Google trends to proxy the prevailing sentiment. Our result has some likeness to the results reported by Florackis et al. (2023) and Tosun (2021). However, the proxies have varying

explanatory power in each of the test windows but none of the four have the ability to explain the market sentiment in all the test windows.

Total assets (both the first and second degree terms) are significant at the 10% level in the announcement window (0,0). The first degree term is positive and the second degree term is negative, implying the presence of a quadratic relationship with a local maximum. The positive relationship between the first degree total asset terms and the returns in event windows surrounding the announcement are supported by multiple prior studies (Florackis et al. (2023), Kamiya et al. (2021), Ettredge et al. (2018), and Lending et al. (2018)). We report that the impact on the CAR increases at an increasing rate with an increase in the asset size, however when the firm's asset increases beyond 40 million USD the impact on the CAR increases at a decreasing rate. Arguably, this may be due to increasing sophistication in the firm's security measures and preparedness to initiate remedial or counter measures in an event of a breach.

The parent breach dummy is negative and the significance increases to 5% from 10% as we traverse from the announcement window (-1,+1) to the post announcement window (+1,+1). However the CAR increase by ~10 bps as the firm move from the announcement window to the post announcement window, this apparent increase can be attributed to the ability and the resourcefulness of an ultimate parent to handle adverse shocks. We report a similar trend in the number of records affected in the cybersecurity incident with increasing significance across the test windows, however the impact on the CAR is fairly uniform. The severity dummy for a breach is associated with a CAR reduction of 88.9 bps. The variable is only significant in the announcement window (0,0); however, the significance is very strong at the 1% level. We can

conclude that the impact is driven entirely by the market forces based on their estimation of the losses due the increased operational and reputation risk for the affected firm.

Examining the sectoral impacts, Ettredge et al. (2018), Gatzert and Schubert (2022), Heidinger and Gatzert (2018), and Kamiya et al. (2021) have analysed the impact of cyber-attacks on different sectors however these studies often group two or more major industry sector (one possible reason maybe due to shortfall in their respective sample size). For instance, Gatzert and Schubert (2022) and Heidinger and Gatzert (2018) focus entirely on the financial sector, while Kamiya et al. (2021) examine three groups, 1) retail and wholesale trade, 2) services, and 3) transportation and utility. We build on these studies by analysing all the major industry sector. The results of the univariate analysis for the retail trade and the wholesale trade are further reinforced, we observe a strong adverse impact in the test windows immediately preceding the announcement (ranging from -100 bps to -200 bps with weak to strong significance), the impact somewhat reduces in the test windows surrounding the announcement. However, in the test windows immediately following the announcement the impact persists and also slightly increases in some of the test windows. We postulate that the firms' higher degree of dependence on their digital infrastructure enables investors to anticipate the potential losses due to the cybersecurity incident before an official announcement. The apparent recovery can be attributed to the remedial and counter measure announced with the breach disclosure, however in the test windows following the announcement the market forces correct for any additional adverse effects to the firm due to their increased operational and reputational risk.

The impact on the CARs for the firms in the utility, manufacturing, transportation, finance and services sector are insignificant in the test windows immediately preceding the

announcement or the test windows including the announcement itself. However, in the test windows following the announcement windows ((+1,+1) and (+1,+2)) we report strongly significant impact on the CARs at the 10% level with the impact ranging from approx. -90 bps to -200 bps. Arguably, this maybe due to the importance of the digital infrastructure in their day-to-day operations and even a single compromised module in the infrastructure can lead to business interruption. Furthermore, we can postulate that the large adverse impact is due to investors penalising the firms for both the business interruption and the subsequent cost incurred to address the compromised module and stakeholders. It is noteworthy that the construction sector yields insignificant results, this can be due to two reasons, 1) the construction sector is the least represented in the sample and 2) the sector is less reliant on the digital infrastructure and the breach don't interfere with their business operations.

Finally, we examine whether different types of breaches cause differential stock price reactions. In contrast to our univariate analysis, the impact due to stolen card information is insignificant, arguably due to them being perceived as low risk. This perceived lower riskiness can be attributed to: 1) the ease of monitoring and reporting any unusual transactions by cardholders, and 2) improvement in the methodology to identify and flag suspicious transactions by the issuing firm. Firm's private information can be compromised in one of two ways, by means of unintended disclosure by an executive or an insider intentionally disclosing information for material gain. Both data breach methods have a strongly significant (5% level) adverse effect on the firm in day t-1. However unintended disclosure is insignificant in days t, t+1 and t+2 while data leak due insider leak show signs of recovery in days t+1 and t+2. This difference in investor behaviour can be attributed to the relatively lower riskiness contained in the information disclosed unintentionally,

by contrast a data leak by an insider have more adverse effects. Furthermore, it is relatively easier to identify the records compromised by an insider. Enabling the firms to take a pinpointed remedial measure, thus recovering some of the lost investor confidence. Data breach due to theft of stationary and portable device have strong adverse effects (significant at the 5% level) in the test window surrounding the announcement. The impact on CAR for theft of stationary device is more than twice the impact on the CAR for the theft of portal devices, this is on expected lines since the volume of data available on a stationary device such as a server or mainframe is much higher than the data available on laptop or other handheld devices.

Regression Analysis – Conditional Analysis Model

We try to further disentangle the impact from a cyber-attack by: 1) taking into account the size of the firm on the sentiment proxies, 2) the industrial sector given that the affected firm is the parent, and 3) the nature of the breach given that the affected firm is the parent.

*** Insert Table 7 ***

Table 7 tabulates the results of the regressions for the each of the six test windows in all three event windows. We examine each of the sentiment proxies while accounting for the firm's size in the search trends. We report a slight increase in the predictive power only for the cybersecurity index in the days leading up to the announcement and the data breach index in the days following the announcement. However, similar to the results in the base model the power of the indices is still low despite the inclusion of firm size-scaled sentiment proxies. The first and second degree terms of the natural logarithm of the total assets, the number of records impacted, the severity dummy and the connected event dummy are impacts very similar to the base model.

Analysing the sectoral impacts with the condition of parent breach, we can see that ultimate parent in the construction sector continue to remain insignificant. However, it interesting to note that, the CARs of the ultimate parent in all the remaining sectors have stronger or equivalent significance in the test windows surrounding the announcement and days immediately following the announcement. Moreover, the adverse effects on the CARs deepen further by at least 300 bps and in some cases the detrimental impact is as high as -3,000 bps. Finally, the impact increasingly worsens as we traverse from day t to day t+1 to day t+2. We hypothesis that this apparent penalty imposed by the market is due to higher expectation from the investor to take more proactive preventive measures rather than the reactive remedial measures.

In contrast, imposing the conditionality on the nature of the breach we observe that the signs of recovery in the days following the announcement of the breach. The unconditional terms have same direction and significance as described by the base model, however the impact on the CARs become more adverse. Theft of stationary devices have the strongest impact on the CARs with an impact of -320 bps in day t, -345 bps in day t+1, and -524 bps in day t+2. Contrary to this overall impact the CAR for the parent is -35 bps in day t, +40 bps in day t+1 and day t+2. Arguably this apparent recovery in the investor confidence is due the ability and resourcefulness of a parent to deploy remedial measures more effectively and in a timely manner. However, this extreme adverse impact could also be due to the number of such incidents in the sample. We have 19 instances of data breach due to theft of stationary devices, 18 of which involve parents. Data breaches due to an insider have a similar impact on the CARs as data breaches involving theft of stationary devices but the impact is relatively weaker when compared to the latter. The impact on the CARs weakens further for data breach due to unintentional disclosure by executives,

however the relative changes in the impact as we traverse from day t to day t+2 is similar to that of theft of stationary devices. It is noteworthy that although theft of transaction card lacks significance in the base model, imposing the conditionality of ultimate parent being affected by this breach type, we report an adverse effect on the CARs on day t. This finding reinforces the univariate analysis of the breach type with the parent driving the entire impact on the CAR. Imposing the conditionality on the hacking breach type yield no additional information relative to the base model or the univariate analysis.

Overall, in general the investors penalise ultimate parents more severely in the event of a data breach vis-à-vis a subsidiary. However, the parents are able to recover a portion of the investor confidence with some of the remedial and future preventive measure for the specific breach types but this recovery is absent in the event of a breach in the subsidiary.

Logistic Regression Analysis – Estimating a Firm's Susceptibility to Cybersecurity Incidents

We estimate a firm's probability of becoming a target to a cyber-attack by comparing our treatment sample of firms that became victims of cyber-security attacks/ data breaches to a control sample of unaffected firms. The control group is obtained by one-to-one matching based on the preceding year's market value, industry sector, and year. A tolerance value of 0.5 (±50%) is set for the market value of the control group against the market value of the test group. For our sample of 728 ultimate parents, enforcement of these criteria provides matches for 460 ultimate parents.

*** Insert Table 8 ***

Table 8 presents the impact of various factors on the likelihood of a cyber-security incident. These factors include 1) sentiment proxies, 2) the natural logarithm (first and second degree) of total assets, 3) first and second degree net income (in USD million), 4) cash and short-term investments (in USD million), and 4) sentiment proxies scaled by firm size. The first column tabulates the parameter estimates of the logistic regression; the corresponding odds ratios are in the second column. Cash and other short term investments, the investor sentiment proxies, and the interaction terms of the firm size and the proxies all lack significance. We report the first and second degree terms of a firm's asset size exhibit strong significance at the 5% level. The first degree term for net income is strongly significant at the 5% level, and the second degree term is significance at the 1% level.

At the same time, contrary to the findings for Lending et al. (2018), the first degree parameter estimate of assets is positive. Furthermore, the second degree parameter estimate is negative. By contrast, the first degree parameter estimate of assets is positive, and the second degree parameter estimate is negative. Figure 3 provides a graphical representation of those relationships, showing a convex relationship between the likelihood of a cyber-attack and firm size that reaches its apex at $52.98 million USD. In contrast, we observe a concave relationship between the probability of a cyber-attack and net income, with the lowest probability occurring at a net income of $3.72 million USD. We argue that firms with assets below this threshold are less interesting for hackers as a target due to their limited resources to pay ransoms or fewer monetizable records, while firms with assets above this threshold have adequate resources to defend themselves against a cyber-attack. Interpreting the relationship between net income and the likelihood is more nuanced, since the likelihood of a cyber-attack increases on both sides of

the threshold. We postulate that since the right tail of the curve represents higher income, it corresponds to a heightened probability of cyber-attacks due to firms' potentially greater attractiveness as targets, while the left tail, associated with lower income, firms may invest less in security measures and thus have a heightened vulnerability to cyber-attacks. Finally, it is noteworthy that all odd ratio estimates are extremely close to 1 with the exception of the first degree total assets variable.

*** Insert Figure 3 ***

VII. Conclusion

Cyber-security incidents or data breach events have an incontestable adverse effect on a firm's stock price. Despite the similarity in their end results (loss of the firm's, its employees', or its customers' electronic data), not all cyber-security incidents have the same effect on the stock price of the firm. In this paper, we try to differentiate and explain the forces driving the abnormal returns around corporate revelations of cyber-attacks. To account for the various forces driving the abnormal returns, we classify cyber-security incidents based on the mechanisms used to launch the attack, and categorize firms based on their industry sectors and variables that proxy for the prevailing investor sentiment. We conclude that different types of cyber-security incidents have different impacts, with some affecting market value prior to an announcement being made about the attack and some extending further after the announcement is made.

We proxy for prevailing investor sentiment by examining differences in the search popularity of a given search term at the start of the week leading up to the incident to the end of the week following its announcement. In our analysis, none of the four proxies (differential

Google search trends for cybercrime, cyber-security, data breach, and firm name) show significance across all of the test windows, although we do find that each proxy has significance in one or more of the test windows. We conclude that although the proxies have some explanatory power, and although we try to improve the explanatory power by controlling for firms' asset sizes, the improvement in explanatory power is still inadequate.

Data breaches resulting from theft of a stationary device have the strongest adverse impact on a firm's stock price, and only a parent can forgo some of the abnormal returns approximately t+2 days after the incident. Intentional data leaks from an insider, on the other hand, have an adverse impact on the abnormal return prior to the incident's announcement, but firms can overcome the adversity somewhat sooner. We conclude that this is due to remedial measures announced along with the incident. Unintended disclosure and theft of portable devices have the lowest impact on abnormal returns, with the effect present only in the period preceding the event's announcement. This can in part be explained by the lower volume of the data lost in the breach. We report a similar response to stolen bank card information; technological advancements have enabled consumers to block compromised transaction cards and have given financial institutions the ability to identify and reverse fraudulent transactions. An unexpected result in our analysis is the lack of negative abnormal returns in the event of a third-party hack. This idiosyncracy can be attributed to 1) the definition of the variable in our study, as our definition includes all third-party interference such as phishing, malware, viruses, software intrusion, DDoS attacks, ransomware etc., and 2) the possibility that a firm affected by a major hacking incident may withhold disclosing the extent of its impact to address and assist ongoing investigations and remedial measures.

Our sectoral analysis yields strong results on days t, t+1, and t+2 after the announcement in the utility, manufacturing, transportation, wholesale trade, retail trade, finance, and services and no results in the period preceding the announcement. Furthermore, contrary to the analysis on the nature of cyber-attack, the conditional analysis for an ultimate parent on the CAR shows an increasing adverse impact for all the sectors. This can be attributed to two factors: 1) although these firms are better equipped to handle a cyber-attack, their investors expect better preventive measures rather than remedial measures, and 2) ultimate parent entities have more at stake than their subsidiaries. This is also evident with day t+2 having a stronger adverse impact on CARs by up to 80 bps when compared to the CARs on day t+1. Furthermore, unlike the nature of breach, particularly unintended disclosure, theft of stationary devices, and leak by insiders, we do not observe recovery in the days following the announcement. Maximum impact on the abnormal return is observed in the wholesale trade sector, followed by retail trade, followed by finance, services, and transportation, and finally by utilities. These results are as anticipated, since the operation of each of these sectors directly affects the day-to-day life of consumers. Finally, parents themselves have a strong adverse impact on the CARs in both the windows including the announcement day and the windows post–announcement day. We can interpret this as investors' acceptance of the remedial measures to the breach, however the firm itself continues to be penalised for the cybersecurity incident.

We estimate the probability of a cyber-attack on a firm by including a control group of comparable market value in the preceding fiscal year and operating in the same sector as the test group. The proxies of the prevailing inventor sentiment lack explanatory power for determining the probability of a cyber-attack, and controlling for the sentiment based on the firm's asset size

has no effect either. However, the probability of a cyber-attack attack has a convex relationship with asset size, while the net income has a concave relationship with the probability of a cyber-attack. We conclude that increasing asset size beyond the local maximum enhances the firm's ability to enforce preventive measures. By contrast, increasing net income levels beyond the local minimum increases the firm's attractiveness as a target, and net income below the threshold may be associated with fewer security measures to prevent cybersecurity attacks. The limiting threshold for assets is $53.98 million USD and for net income is $3.72 million USD.

With the strong empirical results in the univariate analysis, which were further reinforced with a regression analysis, we can confidently conclude that different cyber-security incidents lead to different market responses. While some generate no response, others can lead to abnormal returns that are as high as -600 basis points. Though our study did encounter limitations in terms of sample size and the proxy for investor sentiment, it also opens several avenues for future research. Analysing each threat individually, especially hacking or cyber disruptions due to a third party, could be an interesting avenue to consider in future studies.

VIII. References

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989. https://doi.org/10.1016/j.jfs.2022.100989

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis*, *65*, 101386. https://doi.org/10.1016/j.irfa.2019.101386

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432–448. https://doi.org/10.1016/j.jfineco.2022.12.002

Cummins, J. D., Lewis, C. M., & Wei, R. (2006). The market value impact of operational loss events for US banks and insurers. *Journal of Banking & Finance*, *30*(10), 2605–2634. https://doi.org/10.1016/j.jbankfin.2005.09.015

Eling, M., & Jung, K. (2022). Heterogeneity in cyber loss severity and its impact on cyber risk measurement. *Risk Management*, *24*(4), 273–297. https://doi.org/10.1057/s41283-022-00095-w

Eling, M., & Loperfido, N. (2017). Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics*, *75*, 126–136. https://doi.org/10.1016/j.insmatheco.2017.05.008

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, *25*(2), 383–417. https://doi.org/10.2307/2325486

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity Risk. *The Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725–763. https://doi.org/10.1111/jori.12381

Heidinger, D., & Gatzert, N. (2018). Awareness, determinants and value of reputation risk management: Empirical evidence from the banking and insurance industry. *Journal of Banking & Finance*, *91*, 106–118. https://doi.org/10.1016/j.jbankfin.2018.04.004

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the Impact of Successful Cyberattacks on Target Firms?* (Working Paper 24409). National Bureau of Economic Research. https://doi.org/10.3386/w24409

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate Governance, Social Responsibility, and Data Breaches. *Financial Review*, *53*(2), 413–455. https://doi.org/10.1111/fire.12160

MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, *35*(1), 13–39.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256–286. https://doi.org/10.1002/pam.20567

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

Welburn, J. W., & Strong, A. M. (2022). Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*, *42*(8), 1606–1622. https://doi.org/10.1111/risa.13715

Westland, J. C. (2020). The information content of Sarbanes-Oxley in predicting security breaches. *Computers & Security*, *90*, 101687. https://doi.org/10.1016/j.cose.2019.101687

Figures

Figure 1: Sample Construction Process.

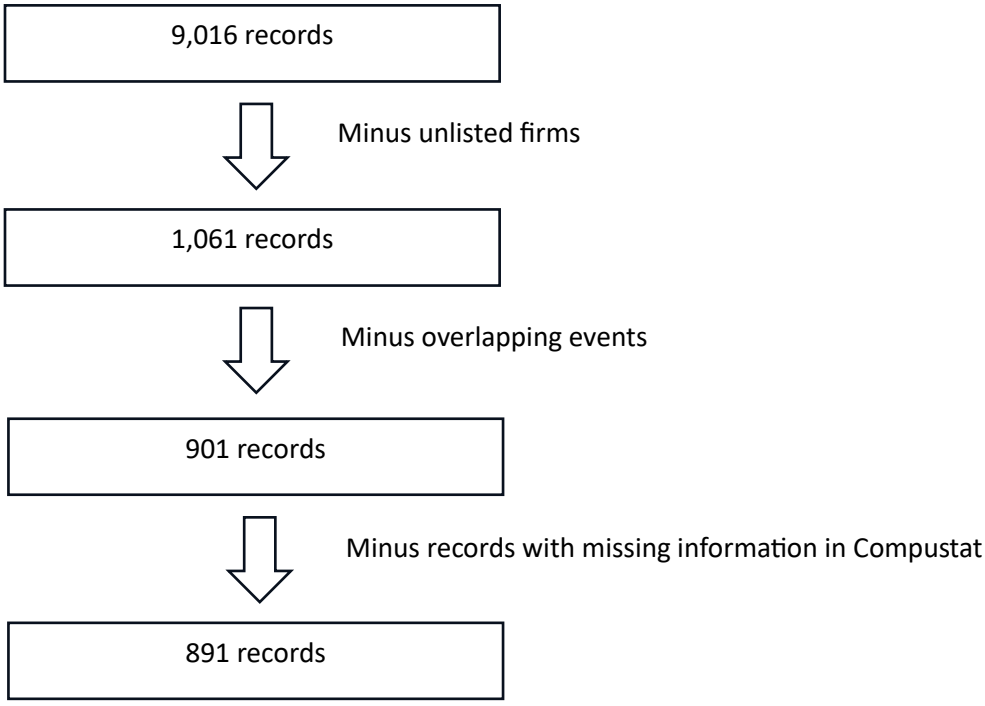
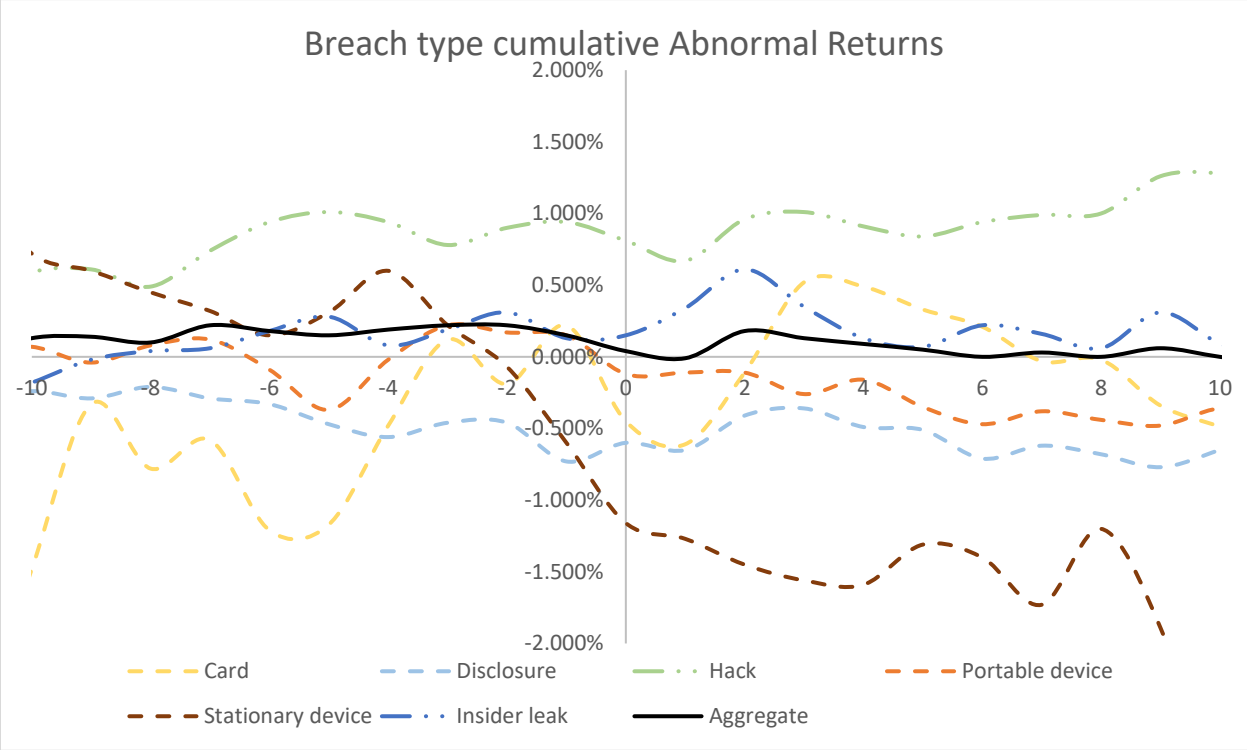
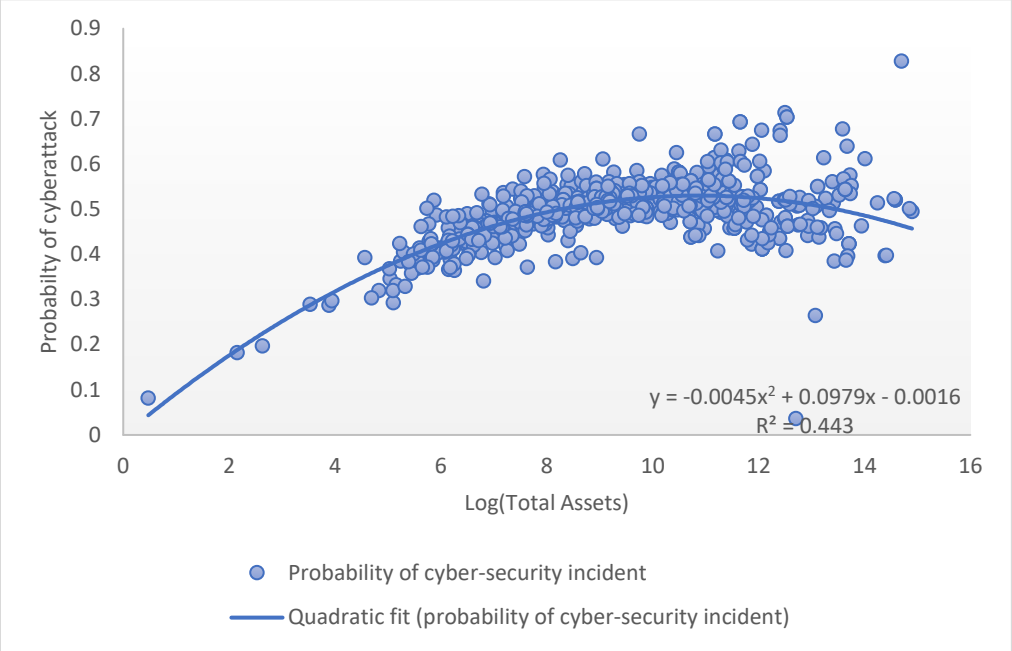


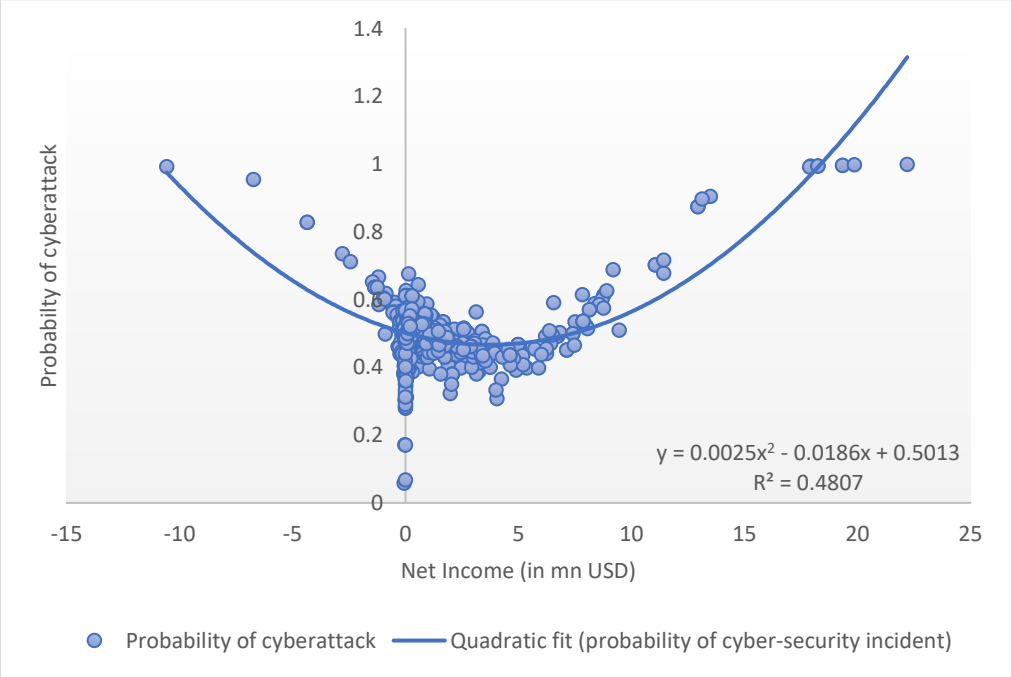
Figure 2: CARs For Different Types Of Cyber-security Incidents And The Overall Sample



Note: *Cyber-security incidents with negative CARs are given heavier line weights compared to cyber-security incidents with positive CARs. The overall sample is represented by a solid line. The positive abnormal returns after a hack may be unrepresentative and influenced by the fact that in this study a hack is defined as a third-party intrusion in a firm's systems and network, which includes phishing, malware, DDoS attacks, ransomware etc. The severity of each intrusion varies, and the difference is further exasperated by delays in announcements (in accordance with the breach notification laws), diluting the overall impact on the abnormal returns.*

Figure 3: Probability Distribution Of A Cyber-security Incident Relative To A Firm's Asset Size And Net Income





Note: The likelihood of cyber-security incidents reaches its maximum at an asset size of $52.98 mn USD; the likelihood decreases if the asset size is either lower or higher than that value. In comparison, the likelihood of a cyber attack is minimal when a firm's net income is $3.72 mn USD and increases when the firm's net income is lower or higher than that value.

Tables

Table 1: Summary statistics

The table provides summary statistics for our sample of 891 data breach incidents involving publicly traded US corporations between January 1, 2005, and February 28, 2019, reported by the Privacy Rights Clearing House (PRC).

Year	Total records lost (in millions)	Number of events	Card information leaked	Unintended disclosure	Network hacked	Theft of portable devices	Theft of stationary devices	Insider information leaked	Unknown breach
2005	12.06	27	0	4	0	15	2	5	1
2006	5.64	72	1	9	5	43	5	8	1
2007	134.97	74	0	11	11	39	2	9	2
2008	16.3	40	1	4	6	21	3	4	1
2009	1.73	19	2	4	2	5	1	5	0
2010	102.12	78	5	18	14	10	2	21	8
2011	358.95	66	6	16	11	11	1	15	6
2012	200.39	79	3	13	23	11	1	25	3
2013	59.82	78	4	21	26	10	2	8	7
2014	285.1	95	1	27	49	2	0	14	2
2015	80.57	43	0	14	23	2	0	3	1
2016	4,120.84	53	0	17	34	2	0	0	0
2017	260.45	58	0	16	41	1	0	0	0
2018	608.76	104	0	12	22	0	0	2	68
2019	0.47	5	0	4	1	0	0	0	0
Total	6,248.25	891	23	190	268	172	19	119	100

Table 2: Variable definitions

Variable	Description
Cybercrime Index	Cybercrime vulnerability index proxied by differential Google search trend. Since Google trends annual search reports the weekly search trends scaled by the maximum searches in the year, we calculate the differential search trend as the difference between the searches at the start and end of the week leading to the cyber-security incident
Cyber-security Index	Cyber-security vulnerability index proxied by differential Google search trend. The differential search trend is calculated similar to Cybercrime Index.
Data Breach Index	Data breach vulnerability index proxied by differential Google search trend. The differential search trend is calculated similar to Cybercrime Index.
Firm Breach Index	Firm breach vulnerability index proxied by differential Google search trend. The differential search trend is calculated similar to Cybercrime Index.
Log (Total Assets)	Natural logarithm of the firm's total assets
Cybercrime Index x Log (Total Assets)	Interaction term between cybercrime sentiment and total assets
Cyber-security Index x Log (Total Assets)	Interaction term between cyber-security sentiment and total assets
Data Breach Index x Log (Total Assets)	Interaction term between data breach sentiment and total assets
Parent Breach	Parent dummy, equal to 1 if the entity is an ultimate parent and zero otherwise
Records	Reported total records lost due to the breach
Breach Severity	Breach dummy, equal to 1 if the total records lost is greater than ten million and zero otherwise
Connected	Breach dummy, equal to 1 if the data breach affected more than one entity and zero otherwise
Utility	Sector dummy, equal to 1 if the entity belongs to the communications, electricity, power, and water distribution sector and zero otherwise
Construction	Sector dummy, equal to 1 if the entity belongs to the construction sector and zero otherwise
Manufacturing	Sector dummy, equal to 1 if the entity belongs to the manufacturing sector and zero otherwise
Transportation	Sector dummy, equal to 1 if the entity belongs to the transportation sector and zero otherwise
Wholesale Trade	Sector dummy, equal to 1 if the entity belongs to the wholesale trade sector and zero otherwise
Retail Trade	Sector dummy, equal to 1 if the entity belongs to the retail trade sector and zero otherwise
Finance	Sector dummy, equal to 1 if the entity belongs to the finance sector and zero otherwise
Service	Sector dummy, equal to 1 if the entity belongs to the service sector and zero otherwise
Card	Breach dummy, equal to 1 if the breach was due to stolen card information and zero otherwise
Disclosure	Breach dummy, equal to 1 if the breach was due to unintended disclosure by the firm and zero otherwise

Variable	Description
Hacked	Breach dummy, equal to 1 if the breach was due to the firm's network or systems being disrupted and zero otherwise
Portable Device	Breach dummy, equal to 1 if the breach was due to stolen portable devices belonging to the firm and zero otherwise
Stationary Device	Breach dummy, equal to 1 if the breach was due to stolen stationary devices belonging to the firm and zero otherwise
Insider Information	Breach dummy, equal to 1 if the breach was due to material information intentionally sold or released by an insider and zero otherwise
Parent Breach x Utility	Interaction term to capture the impact of the ultimate parent in the public utility sector being breached
Parent Breach x Construction	Interaction term to capture the impact of the ultimate parent in the construction sector being breached
Parent Breach x Manufacturing	Interaction term to capture the impact of the ultimate parent in the manufacturing sector being breached
Parent Breach x Transportation	Interaction term to capture the impact of the ultimate parent in the transportation sector being breached
Parent Breach x Wholesale Trade	Interaction term to capture the impact of the ultimate parent in the wholesale trade sector being breached
Parent Breach x Retail Trade	Interaction term to capture the impact of the ultimate parent in the retail trade sector being breached
Parent Breach x Finance	Interaction term to capture the impact of the ultimate parent in the finance sector being breached
Parent Breach x Service	Interaction term to capture the impact of the ultimate parent in the service sector being breached
Parent Breach x Card	Interaction term to capture the impact of card information stolen from the parent organization
Parent Breach x Disclosure	Interaction term to capture the impact of unintended disclosure by the parent organization
Parent Breach x Hacked	Interaction term to capture the impact of the parent organization being hacked
Parent Breach x Portable Device	Interaction term to capture the impact of theft of portable devices belonging to the parent organization
Parent Breach x Stationary Device	Interaction term to capture the impact of theft of stationary devices belonging to the parent organization
Parent Breach x Insider Information	Interaction term to capture the impact of material information intentionally sold or released by an insider from the parent organization

Table 3: Correlation matrix

We report Pearson/Spearman correlation coefficients for each variable pair. The symbol * denotes statistical significance of 10% or stronger.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Cybercrime Index	1	1																						
Cybersecurity Index	2	0.15	1																					
Data Breach Index	3	0.1*	0	1																				
Firm Search Index	4	0	0.04	0.03	1																			
Log (Total Assets)	5	0.04	0.03	0.03	0.03	1																		
Parent Breach	6	0.05*	-0.03	-0.01	-0.05	0	1																	
Records	7	-0.01	0	-0.06*	0	0	0.01	1																
Severity	8	-0.03	0.05	0	-0.01	-0.02	0	0.37	1															
Connected	9	0	0.02	-0.09*	-0.01	0.04	0.01	-0.01	-0.03	1														
Utility	10	-0.02	-0.02	0	0.06*	0.1*	-0.08*	0	0.04	-0.04	1													
Construction	11	-0.01	-0.04	-0.01	-0.05	-0.05*	-0.01	0	-0.01	-0.02	-0.01	1												
Manufacturing	12	0.03	0.03	-0.01	0.06*	-0.08*	0.06*	-0.02	-0.03	0.02	-0.1*	-0.02	1											
Transportation	13	0.02	-0.01	0.03	-0.06*	-0.01	-0.06*	-0.01	-0.02	-0.05	-0.03	-0.01	-0.06*	1										
Wholesale Trade	14	0	-0.03	-0.03	-0.03	-0.07*	-0.05*	0	-0.01	-0.03	-0.02	0	-0.04	-0.01	1									
Retail Trade	15	-0.03	-0.04	0.02	0.07*	-0.19	0.06*	-0.01	0.02	-0.01	-0.09*	-0.02	-0.17	-0.06*	-0.04	1								
Finance	16	0.03	0.02	0	-0.06*	0.41	0	-0.04	-0.08*	0.04	-0.19	-0.05	-0.34	-0.12*	-0.08*	-0.32	1							
Services	17	-0.04	0.01	0	-0.04	-0.3	-0.02	0.09*	0.11*	-0.01	-0.12*	-0.03	-0.21	-0.07*	-0.05	-0.2	-0.4	1						
Card	18	0.01	0	0	0	0.13	0.04	-0.01	-0.02	0.06*	-0.03	-0.01	-0.03	-0.02	0.04	0	0.09*	-0.06*	1					
Disclosure	19	0.04	-0.03	0.01	0.02	0.06*	0.01	-0.03	-0.05*	0	-0.01	-0.03	-0.09*	-0.01	-0.02	-0.02	0.1*	0	-0.08*	1				
Hacked	20	-0.02	0.02	-0.04	-0.01	-0.15	-0.1*	0.09*	0.2	-0.05	0.03	0	0.06*	0.02	0.04	0.01	-0.23	0.17	-0.1*	-0.34	1			
Portable Devices	21	0	0	0.02	0.02	0	0	-0.03	-0.06*	0.07*	0.05*	-0.03	0.14	-0.04	0	-0.07*	-0.01	-0.08*	-0.07*	-0.25	-0.32	1		
Stationary Device	22	-0.03	-0.04	0.01	-0.03	0.01	0.05	0	-0.02	0.05	-0.03	0.1*	0	0.02	-0.01	-0.03	0	0.02	-0.02	-0.07*	-0.09*	-0.07*	1	
Insider Information	23	0	0.06*	0	0	0.1*	0.03	-0.02	-0.06*	-0.01	0.02	-0.02	-0.07*	0	-0.01	0.08*	0.05*	-0.07*	-0.06*	-0.2	-0.25	-0.19	-0.05*	1

Table 4: Mean cumulative abnormal returns

We report the mean and median cumulative abnormal returns (CARs) for several windows surrounding a given data breach event. The breach events are classified based on their relative proximity to the public announcement date: 1) after the breach but before the breach announcement, 2) time windows that include the announcement day, 3) post breach windows that exclude the announcement day, and 4) other windows. We test for the significance of the abnormal returns using a parametric test (Uncorrected Patell Z) and a non-parametric test (Generalised Sign Z). The symbols *, **, and *** denote statistical significance at the 10%, 5%, and 1% level, respectively.

Event Window	N	Mean Cumulative Abnormal Return	Median Cumulative Abnormal Return	Uncorrected Patell Z	Generalized Sign Z
Panel A: Event Window					
(-1,0)	891	-0.15%	-0.10%	-2.927**	-1.1940
(0,+1)	891	-0.19%	-0.08%	-2.295*	-0.4500
(0,0)	891	-0.10%	-0.05%	-1.974*	0.7920
(-1,+1)	891	-0.24%	-0.20%	-3.124***	-2.936**
Plane B: Pre-Event Window					
(-3,-2)	891	-0.01%	-0.05%	-0.2370	-0.4560
(-2,-1)	891	-0.08%	-0.12%	-1.860*	-0.6580
Panel C: Post-Event Window					
(+1,+2)	891	0.12%	0.06%	1.0550	1.621*
(+2,+3)	891	0.19%	0.08%	2.234*	2.560**
Panel D: Other Windows					
(-3,0)	891	-0.16%	0.08%	-2.238*	-0.859
(-2,0)	891	-0.18%	0.08%	-2.658**	-1.730*
(0,+2)	891	0.03%	0.08%	-0.278	1.688*
(0,+3)	891	0.00%	0.08%	-0.043	0.75
(-3,+3)	891	-0.06%	0.08%	-0.978	0.147
(-2,+2)	891	-0.05%	0.08%	-1.392*	0.482

Table 5: Univariate analysis

We construct several subsamples along various dimensions and compare the mean and median CARs between various subsample pairs. In particular, we explore the impact of various characteristics against the remainder of the sample (based on asset size, firm sectors, and the nature of the data breach / cyber-security threat). In addition to these characteristics, we evaluate their impact in different event windows (Announcement Window (0,0) and Pre-Announcement Window (-2,-1)). For each sample, we report N (the number of firms), Mean (the cumulative abnormal return), and Median (the median cumulative abnormal return). We test for the significance of differences between mean and median returns between samples using a parametric 2 sample t-test for the difference in means and a non-parametric median test for the difference in medians. We report the p-value for each test. The symbols *, **, and *** denote statistical significance at the 10%, 5%, and 1% level, respectively.

Subsample 1	N, Mean, Median	Subsample 2	N, Mean, Median	Test of Differences Means (p-value), Medians (p-value)
Panel A: Ranked by Asset Size				
CAR (0,0) First quintile	178	CAR (0,0) Fifth quintile	178	
	-0.4187		-0.2908	0.4676
	-0.27		0.1	0.102
CAR(-2,-1) First	178	CAR(-2,-1) Fifth	178	
quintile	0.0122	quintile	-0.0952	0.6606
	-0.32		-0.095	0.102
Panel B: Finance Sector				
CAR (0,0) Finance	354	CAR (0,0) All firms	537	
Sector	-0.1451	except Finance	-0.1227	0.8296
	0.01		-0.1	0.1122
CAR(-2,-1) Finance	354	CAR(-2,-1) All firms	537	
Sector	-0.0645	except Finance	-0.1832	0.4014
	-0.01		-0.14	0.2384
Panel C: Construction Sector				
CAR (0,0) Construction	4	CAR (0,0) All firms	887	
Sector	-0.2525	except Construction	-0.1311	0.8733
	-0.71		-0.05	0.4991
CAR(-2,-1)	4	CAR(-2,-1) All firms	887	
Construction Sector	0.3125	except Construction	-0.1381	0.6633
	-0.16		-0.12	0.4991
Panel D: Manufacturing Sector				
CAR (0,0)	138	CAR (0,0) All firms	753	
Manufacturing Sector	-0.0386	except Manufacturing	-0.1487	0.4336
	-0.085		-0.05	0.4321
CAR(-2,-1)	138	CAR(-2,-1) All firms	753	
Manufacturing Sector	-0.063	except Manufacturing	-0.1494	0.6515
	-0.28		-0.08	0.2339

Subsample 1	N, Mean, Median	Subsample 2	N, Mean, Median	Test of Differences Means (p-value), Medians (p-value)
Panel E: Transportation Sector				
CAR (0,0)	22	CAR (0,0) All firms	869	
Transportation Sector	-0.1682	except Transportation	-0.1307	0.909
	-0.37		-0.04	0.1952
CAR(-2,-1)	22	CAR(-2,-1) All firms	869	
Transportation Sector	-0.1123	except Transportation	-0.1366	0.9564
	0.175		-0.12	0.3311
Panel F: Wholesale Trade Sector				
CAR (0,0) Wholesale	10	CAR (0,0) All firms	881	
Trade Sector	-0.237	except Wholesale	-0.1304	0.8254
	-0.6	Trade	-0.04	0.1021
CAR(-2,-1) Wholesale	10	CAR(-2,-1) All firms	881	
Trade Sector	-2.151	except Wholesale	-0.1132	0.0019***
	-1.975	Trade	-0.09	0.0056***
Panel G: Retail Trade Sector				
CAR (0,0) Retail Trade	125	CAR (0,0) All firms	766	
Sector	-0.2831	except Retail Trade	-0.1069	0.229
	-0.12		-0.03	0.2539
CAR(-2,-1) Retail Trade	125	CAR(-2,-1) All firms	766	
Sector	-0.4378	except Retail Trade	-0.0868	0.0779*
	-0.18		-0.08	0.1965
Panel H: Service Sector				
CAR (0,0) Service	178	CAR (0,0) All firms	713	
Sector	-0.1683	except Service	-0.1225	0.7187
	-0.125		-0.03	0.1022
CAR(-2,-1) Service	178	CAR(-2,-1) All firms	713	
Sector	-0.1257	except Service	-0.1386	0.9403
	0.005		-0.14	0.1965
Panel I: Utility Sector				
CAR (0,0) Utility Sector	49	CAR (0,0) All firms	842	
	0.2078	except Utility	-0.1514	0.1074
	0.16		-0.065	0.0274**
CAR(-2,-1) Utility	49	CAR(-2,-1) All firms	842	
Sector	0.23	except Utility	-0.1573	0.2016
	-0.12		-0.115	0.4448
Panel J: Theft of Card Information - Breach Type				
CAR (0,0) Theft of Card	23	CAR (0,0) All breach	868	
information	-0.5157	types except Theft of	-0.1215	0.2191
	-0.53	Card information	-0.035	0.0702*
CAR(-2,-1) Theft of	23	CAR(-2,-1) All breach	868	
Card information	0.097	types except Theft of	-0.1422	0.5835
	-0.18	Card information	-0.115	0.4185

Subsample 1	N, Mean, Median	Subsample 2	N, Mean, Median	Test of Differences Means (p-value), Medians (p-value)
Panel K: Unintended Disclosure - Breach Type				
CAR (0,0) Unintended	190	CAR (0,0) All breach	701	
Disclosure	-0.0618	types except	-0.1505	0.4752
	-0.02	Unintended Disclosure	-0.06	0.3651
CAR(-2,-1) Unintended	190	CAR(-2,-1) All breach	701	
Disclosure	-0.1968	types except	-0.1196	0.6473
	-0.15	Unintended Disclosure	-0.08	0.3181
Panel L: Hacked - Breach Type				
CAR (0,0) Network	268	CAR (0,0) All breach	623	
Hacked	-0.1362	types except Network	-0.1297	0.9696
	-0.06	Hacked	-0.03	0.4123
CAR(-2,-1) Network	268	CAR(-2,-1) All breach	623	
Hacked	-0.0004	types except Network	-0.1943	0.1986
	-0.01	Hacked	-0.17	0.0691*
Panel M: Theft of Portable Devices - Breach Type				
CAR (0,0) Theft of	172	CAR (0,0) All breach	719	
Portable devices	-0.2521	types except Theft of	-0.1028	0.2468
	-0.095	Portable devices	-0.04	0.2536
CAR(-2,-1) Theft of	172	CAR(-2,-1) All breach	719	
Portable devices	-0.2507	types except Theft of	-0.1086	0.4175
	-0.235	Portable devices	-0.08	0.1207
Panel N: Theft of Stationary Devices - Breach Type				
CAR (0,0) Theft of	19	CAR (0,0) All breach	872	
Stationary devices	-0.5484	types except Theft of	-0.1225	0.2265
	-0.34	Stationary devices	-0.03	0.0526*
CAR(-2,-1) Theft of	19	CAR(-2,-1) All breach	872	
Stationary devices	-0.6732	types except Theft of	-0.1243	0.2516
	-0.28	Stationary devices	-0.115	0.4103
Panel O: Insider Information - Breach Type				
CAR (0,0) Insider	119	CAR (0,0) All breach	772	
Information	0.041	types except Insider	-0.1582	0.1827
	-0.015	Information	-0.06	0.221
CAR(-2,-1) Insider	119	CAR(-2,-1) All breach	772	
Information	-0.0861	types except Insider	-0.1437	0.7767
	-0.1	Information	-0.12	0.466

Table 6: Regression analysis for CARs: Base model

We examine whether different cybersecurity incidents lead to different investor responses on the announcement day by regressing the test window CARs against different investor sentiment proxies, a firm's asset size, number of records lost (in millions), the severity of the breach (a dummy variable identifying whether the number of records lost exceeds 10 million), and a series of dummy variables identifying industry sectors and types of cyber-security incidents. Coefficient p-values are reported below the parameter estimate in parenthesis. The symbols *, **, and *** indicate significance at the 10%, 5%, and 1% level, respectively.

	Event Window		Per-Event Window		Post-Event Window	
	(-1,+1)	(0,0)	(-1,-1)	(-2,-1)	(+1,+1)	(+1,+2)
Cybercrime Trend	0.0078	-0.0046	0.0112***	0.0039	0.0007	0.0052
	(0.2802)	(0.2594)	(0.0036)	(0.4856)	(0.8497)	(0.3887)
Cyber-security Trend	-0.002	-0.002	-0.001	-0.004	0.0026	0.0029
	(0.6169)	(0.3909)	(0.6206)	(0.2171)	(0.2446)	(0.401)
Data Breach Trend	-0.0058	-0.001	0	0.0015	-0.0043*	-0.0041
	(0.1956)	(0.6905)	(0.9926)	(0.6554)	(0.0791)	(0.2712)
Firm Search Trend	-0.0104*	-0.0031	-0.0024	-0.0037	-0.0032	0.0003
	(0.0593)	(0.3123)	(0.4116)	(0.3795)	(0.2844)	(0.9461)
Log (Total Assets)	0.3367	0.316*	-0.0864	-0.1549	0.1727	0.0088
	(0.2669)	(0.0669)	(0.5902)	(0.5114)	(0.3008)	(0.9721)
Log (Total Assets)^2	-0.0143	-0.015*	0.0049	0.007	-0.0079	-0.0007
	(0.3316)	(0.0732)	(0.5233)	(0.5389)	(0.3264)	(0.9503)
Parent Breach	-0.3864*	-0.0741	0.029	0.0072	-0.2804**	-0.2096
	(0.0971)	(0.5752)	(0.8136)	(0.9683)	(0.0288)	(0.2819)
Records	-0.0023**	0	0	-0.0002	-0.0016***	-0.0023***
	(0.0126)	(0.9493)	(0.9382)	(0.694)	(0.0017)	(0.003)
Severity	-0.8818	-0.889***	0.0319	-0.3304	0.1596	0.5459
	(0.1332)	(0.0078)	(0.9182)	(0.4693)	(0.6211)	(0.2663)
Connected	-0.1597	-0.1711	-0.0558	0.198	0.145	-0.037
	(0.6138)	(0.3414)	(0.7388)	(0.4212)	(0.4051)	(0.8888)
Utility	-0.5369	0.0649	0.3297	0.4115	-1.127**	-1.8499**
	(0.5487)	(0.8984)	(0.4867)	(0.5546)	(0.0224)	(0.0137)
Construction	-0.5116	-0.378	0.5042	0.4074	-0.6729	-1.0391
	(0.7455)	(0.673)	(0.5457)	(0.7397)	(0.438)	(0.4307)
Manufacturing	-1.1314	-0.1851	0.0615	0.1227	-1.1251**	-1.5327**
	(0.181)	(0.7)	(0.8906)	(0.852)	(0.0158)	(0.0304)
Transportation	-1.3828	-0.3675	0.316	0.1105	-1.379**	-2.5063***
	(0.1696)	(0.5205)	(0.5531)	(0.8877)	(0.0129)	(0.003)
Wholesale Trade	-2.6347**	-0.4868	-1.0619*	-2.3108**	-1.1092*	-0.8177
	(0.0256)	(0.4673)	(0.089)	(0.0119)	(0.0875)	(0.4068)
Retail Trade	-1.6368*	-0.4929	0.0107	-0.3242	-1.1506**	-1.5624**
	(0.0565)	(0.3118)	(0.9812)	(0.627)	(0.0149)	(0.0296)
Finance	-1.2356	-0.3243	0.1673	0.098	-1.09**	-1.6517**
	(0.1334)	(0.4878)	(0.7009)	(0.8782)	(0.0162)	(0.0166)

	Event Window		Per-Event Window		Post-Event Window	
	(-1,+1)	(0,0)	(-1,-1)	(-2,-1)	(+1,+1)	(+1,+2)
Services	-1.0874	-0.296	0.122	0.0175	-0.8936*	-1.5345**
	(0.2001)	(0.5391)	(0.786)	(0.9788)	(0.0559)	(0.0308)
Card	-0.1171	-0.3882	0.0506	0.2609	0.1452	0.7874
	(0.8616)	(0.3096)	(0.8868)	(0.6179)	(0.6946)	(0.1616)
Disclosure	-0.319	-0.0515	-0.4994**	-0.2326	0.2447	0.5313
	(0.4261)	(0.8211)	(0.0188)	(0.4558)	(0.2674)	(0.1133)
Hacked	-0.1892	-0.0523	-0.3086	-0.046	0.1287	0.6672**
	(0.6332)	(0.8162)	(0.1419)	(0.8813)	(0.5553)	(0.0445)
Portable Devices	-0.5195	-0.2758	-0.4885**	-0.4286	0.2305	0.323
	(0.2414)	(0.2737)	(0.0377)	(0.2142)	(0.3448)	(0.3839)
Stationary Devices	-1.3489*	-0.5598	-0.9377**	-0.9033	0.1772	0.0759
	(0.0634)	(0.175)	(0.0149)	(0.11)	(0.6574)	(0.9005)
Insider Information	0.056	0.0627	-0.4968**	-0.0592	0.4372*	0.8747**
	(0.899)	(0.8026)	(0.0338)	(0.8631)	(0.0723)	(0.0181)
Intercept	-0.1329	-0.8437	0.5091	0.4803	-0.0652	1.0917
	(0.9428)	(0.4233)	(0.604)	(0.7391)	(0.949)	(0.4815)
Year Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Adjusted R^2	0.0162	0.0212	0.0362	0.0078	0.0068	0.0273
N	891	891	891	891	891	891

Table 7: Regression analysis for CARs: Conditional analysis

We examine whether different cyber-security incidents lead to different investor responses on the announcement day by regressing the test window CARs against different investor sentiment proxies, a firm's asset size, number of records lost (in millions), the severity of the breach (a dummy variable identifying whether the number of records lost exceeds 10 million), and a series of dummy variables identifying industry sectors given the parent is breached and types of cyber-security incidents. The analysis includes interaction terms of sentiment proxies & a firm's asset size, and firm type & type of cyber-security incident. Coefficient p-values are reported below the parameter estimate in parentheses. The symbols *, **, and *** indicate significance at the 10%, 5%, and 1% level, respectively.

	Announcement Window		Per-Announcement Window		Post Announcement Window	
	(-1,+1)	(0,0)	(-1,-1)	(-2,-1)	(+1,+1)	(+1,+2)
Cybercrime Index	0.0209	-0.0171	0.0243**	0.0068	0.0072	0.0116
	(0.2654)	(0.1096)	(0.0149)	(0.641)	(0.483)	(0.4582)
Cybersecurity Index	-0.0256**	-0.0003	-0.0182***	-0.0135	0.0022	0.0002
	(0.0298)	(0.9608)	(0.0036)	(0.1438)	(0.7332)	(0.9832)
Data Breach Index	-0.0153	0.006	-0.0054	-0.0101	-0.0163**	-0.0256**
	(0.2091)	(0.3802)	(0.3988)	(0.2882)	(0.0145)	(0.012)
Firm Search Index	-0.0261**	-0.004	-0.0101	-0.0113	-0.0093	0.0031
	(0.0308)	(0.5508)	(0.1113)	(0.2305)	(0.1586)	(0.7581)
Log (Total Assets)	0.4187	0.3305*	-0.0245	-0.1148	0.186	-0.0362
	(0.1679)	(0.0558)	(0.879)	(0.6303)	(0.264)	(0.8866)
Log (Total Assets)^2	-0.0185	-0.0157*	0.0018	0.0052	-0.0086	0.0013
	(0.2088)	(0.0602)	(0.8148)	(0.6519)	(0.2831)	(0.9129)
Parent Breach	0.8156	0.0036	0.4702	0.9309	0.4002	0.7813
	(0.5004)	(0.9958)	(0.4637)	(0.3279)	(0.5467)	(0.4405)
Records	-0.0023**	0	0	-0.0001	-0.0016***	-0.0023***
	(0.0124)	(0.9405)	(0.9815)	(0.7849)	(0.0013)	(0.0025)
Severity	-0.8088	-0.8854***	0.0528	-0.2975	0.2111	0.6113
	(0.1664)	(0.0078)	(0.8646)	(0.517)	(0.5101)	(0.2113)
Connected	-0.1367	-0.196	-0.0218	0.2192	0.1523	-0.0392
	(0.6663)	(0.277)	(0.8966)	(0.379)	(0.3813)	(0.8824)
Parent Breach x Utility	-1.8646*	-0.2189	-0.0264	-0.2196	-1.8884***	-2.3568***
	(0.0792)	(0.7168)	(0.9625)	(0.7923)	(0.0012)	(0.0081)
Parent Breach x Construction	-0.9372	-0.6709	0.944	0.5264	-1.2474	-1.8547
	(0.6066)	(0.5169)	(0.328)	(0.7129)	(0.2118)	(0.2235)
Parent Breach x Manufacturing	-2.0503**	-0.3043	-0.2575	-0.3818	-1.5912***	-1.8891**
	(0.0373)	(0.5863)	(0.6212)	(0.6212)	(0.0033)	(0.0219)
Parent Breach x Transportation	-2.2488*	-0.5324	-0.1664	-0.4424	-1.5689**	-2.2878**
	(0.0622)	(0.4372)	(0.7944)	(0.6403)	(0.0178)	(0.0235)
Parent Breach x Wholesale Trade	-3.3829**	-0.91	-1.05	-2.8221**	-1.4176*	-0.697
	(0.0203)	(0.2718)	(0.1738)	(0.0138)	(0.0761)	(0.5672)
Parent Breach x Retail Trade	-2.7888***	-0.7454	-0.2734	-0.7501	-1.725***	-2.1726***
	(0.0053)	(0.1895)	(0.6056)	(0.3393)	(0.0017)	(0.0095)

	Announcement Window		Per-Announcement Window		Post Announcement Window	
	(-1,+1)	(0,0)	(-1,-1)	(-2,-1)	(+1,+1)	(+1,+2)
Parent Breach x Finance	-2.1271**	-0.4796	-0.1081	-0.424	-1.506***	-2.0366**
	(0.0284)	(0.3843)	(0.8333)	(0.5777)	(0.0047)	(0.0122)
Parent Breach x Services	-2.1857**	-0.4893	-0.2412	-0.6887	-1.3963**	-2.0214**
	(0.0279)	(0.3862)	(0.6467)	(0.3775)	(0.0105)	(0.0151)
Parent Breach x Card	-2.6301	-2.2406*	0.0631	0.9233	-0.602	0.2843
	(0.2118)	(0.0616)	(0.9549)	(0.5769)	(0.6023)	(0.8718)
Parent Breach x Disclosure	1.4244	0.4535	-0.2492	-0.5201	1.2238**	1.355*
	(0.1147)	(0.3768)	(0.6024)	(0.4633)	(0.0136)	(0.073)
Parent Breach x Hacked	1.0968	0.4703	-0.1282	-0.3362	0.8252*	1.0172
	(0.1907)	(0.3237)	(0.7728)	(0.6096)	(0.0729)	(0.147)
Parent Breach x Portable Devices	0.5762	0.1202	-0.2932	-0.5357	0.7312	0.4765
	(0.5291)	(0.8174)	(0.5458)	(0.4567)	(0.1457)	(0.534)
Parent Breach x Stationary Device	4.619	2.8598*	-3.0111*	-1.7546	3.8679**	5.6475**
	(0.1132)	(0.0847)	(0.0515)	(0.4436)	(0.0157)	(0.0207)
Parent Breach x Insider Information	1.3671	0.9255	-0.7708	-0.6408	1.0805*	2.1241**
	(0.1772)	(0.1083)	(0.1513)	(0.4208)	(0.052)	(0.0123)
Card	2.3256	1.655	0.0107	-0.6136	0.7176	0.5013
	(0.2515)	(0.1514)	(0.992)	(0.7001)	(0.5188)	(0.7676)
Disclosure	-1.4568*	-0.4307	-0.2345	0.2557	-0.7897*	-0.6516
	(0.0887)	(0.3758)	(0.6049)	(0.7035)	(0.0926)	(0.3625)
Hacked	-1.0526	-0.432	-0.1394	0.2878	-0.5834	-0.2631
	(0.1843)	(0.3379)	(0.74)	(0.644)	(0.1799)	(0.6915)
Portable Devices	-0.9819	-0.3891	-0.2006	0.0385	-0.4055	-0.1458
	(0.2626)	(0.435)	(0.6659)	(0.9553)	(0.3991)	(0.8423)
Stationary Device	-5.6803**	-3.2337**	1.8765	0.6961	-3.4526**	-5.2423**
	(0.0452)	(0.045)	(0.2118)	(0.7546)	(0.0266)	(0.0272)
Insider Information	-1.0474	-0.7332	0.2155	0.5159	-0.4778	-0.9595
	(0.2773)	(0.1812)	(0.6731)	(0.4958)	(0.3662)	(0.2343)
Card	2.3256	1.655	0.0107	-0.6136	0.7176	0.5013
	(0.2515)	(0.1514)	(0.992)	(0.7001)	(0.5188)	(0.7676)
Intercept	-0.8961	-0.9004	0.2	-0.0055	-0.5571	0.5486
	(0.6084)	(0.3655)	(0.8292)	(0.9968)	(0.5616)	(0.7078)
Year Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Investor Sentiment Controls	Yes	Yes	Yes	Yes	Yes	Yes
Adjusted R^2	0.024	0.0275	0.0278	-0.0049	0.0209	0.0181
N	891	891	891	891	891	891

Table 8: Logistic regression analysis for estimation of probability of cybersecurity incident.

We estimate the probability of a cyber-security incident by comparing the test sample against a control group. The control group is obtained by a one-to-one matching of the preceding year's market value and the industry sector for the firms in the test group. A tolerance value 0.5 is set for the market value of control group against market value of the test group. The probability of a cyber-security incident is estimated by regressing the test and control against the firm's asset size, square of the firm's asset size, cash, net income, investor sentiment proxies, and interaction terms of sentiment proxies & a firm's asset size. Coefficient p-values are reported below the parameter estimate in parentheses. The symbols *, **, and *** indicate significance at the 10%, 5%, and 1% level, respectively.

	Logistic Regression	Odds Estimate
Log (Total Assets)	0.5606**	1.752
	(0.0283)	
Log (Total Assets)^2	-0.0267*	0.974
	(0.0589)	
Cash	0.0002	1
	(0.9216)	
Net Income	-0.2028**	0.816
	(0.0221)	
Net Income^2	0.0264***	1.027
	(0.0052)	
CyberCrime Trend	0.0076	1.008
	(0.57)	
Cybersecurity Trend	0.0036	1.004
	(0.6964)	
Data Breach Trend	-0.0082	0.992
	(0.3815)	
Firm search Trend	-0.0005	0.999
	(0.9498)	
Log (Total Assets)^2 x CyberCrime Trend	-0.0059	0.994
	(0.6378)	
Log (Total Assets)^2 x Cybersecurity Trend	-0.0058	0.994
	(0.5241)	
Log (Total Assets)^2 x Data Breach Trend	0.0074	1.007
	(0.4152)	
Log (Total Assets)^2 x Firm search Trend	-0.0059	0.994
	(0.5471)	
Intercept	-2.7325**	
	(0.0171)	
Adjusted R^2	0.0206	
N	920	