Issues in Information Systems
Volume 25, Issue 4, pp. 260-276, 2024

DOI: https://doi.org/10.48009/4_iis_2024_121

Market Reactions to Cybersecurity Incidents: A Case Study Approach

Kevin Day, *Graduate Student, kevin.day@my.metrostate.edu*
Queen Booker, *Associate Professor, queen.booker@metrostate.edu*

Abstract

This paper examines the impact of cybersecurity breaches on the stock prices of publicly traded companies, focusing on notable incidents involving Capital One, Equifax, Facebook, Google, JBS S.A., MGM Resorts International, Nvidia, Okta, SolarWinds, and T-Mobile. Employing event study methodology, we analyze stock price changes relative to the Dow Jones Industrial Average (DJIA) across various time windows surrounding the breach disclosures. Our statistical analysis includes paired t-tests, Wilcoxon signed-rank tests, and correlation analyses to determine the significance and nature of these impacts. Results consistently show statistically significant deviations in stock prices following breach announcements, underscoring the profound financial repercussions. The findings highlight the necessity for robust cybersecurity measures and proactive incident response strategies to mitigate the adverse effects on market performance. This comprehensive study contributes to the understanding of cybersecurity risks and their implications for investor confidence and corporate financial stability, offering valuable insights for stakeholders in managing and responding to cyber threats.

Keywords: cybersecurity breaches, stock prices, financial impact, market reactions, publicly traded companies, data breach analysis

Introduction

In an era of rapid technological advancement, cybersecurity breaches have become a familiar threat across a myriad of industries, highlighting the vulnerabilities inherent to the digital transformation of the business process. As organizations increasingly rely upon digital platforms to conduct their operations, they accumulate vast amounts of sensitive data that, when compromised, can lead to significant disruption. This is particularly true for publicly traded companies whose operations, financial performance, and reputational standing are critically dependent upon their cybersecurity measures. The complexity of modern business ecosystems, with their highly interconnected digital infrastructures, makes understanding the dynamics of cybersecurity breaches crucial.

Background

In the realm of cybersecurity, a data breach refers to the unauthorized or unintended access, disclosure, or acquisition of sensitive or confidential information by an individual, group, or entity. This breach can occur through various means, including hacking, malware attacks, insider threats, or accidental exposure, resulting in the compromise of personal, financial, or proprietary data. The significance of a data breach

lies not only in unauthorized access to sensitive information but also in the potential consequences that may ensue. These consequences can range from financial losses, reputational damage, and legal liabilities to identity theft, fraud, and the erosion of trust among affected individuals or entities. Financial consequences include forensic investigations, customer compensation, and legal fees (Proofpoint, 2023).

A data breach can manifest itself through various means, including the theft of login credentials, exposure of Personally Identifiable Information (PII) such as names, addresses, social security numbers, or financial data, and the compromise of intellectual property, trade secrets, or proprietary business information. Beyond the immediate breach itself, a cascade of repercussions can reverberate throughout an organization or ecosystem.

These include the disruption of business operations, regulatory investigations and penalties, loss of customer trust and loyalty, and potential lawsuits or class-action claims. Understanding the nature, cause, and possible outcomes of data breaches is essential for effective cybersecurity management and risk mitigation strategies in today's interconnected and data-driven landscape (Proofpoint, 2023) (ITRC, 2023)

Particularly vulnerable are industries with stringent regulatory requirements, such as healthcare, which face the highest breach costs at an average of $10.93 million per incident. The Identity Theft Resource Center (ITRC) 2023 report highlights that the healthcare sector has consistently reported the highest number of data compromises over the past five years, emphasizing the need for industry-specific security measures and robust preparedness strategies.

Furthermore, with 82% of breaches involving cloud environments, the data shows especially severe financial impacts when breaches span multiple cloud environments, averaging $4.75 million. These findings emphasize the critical need for comprehensive cloud security frameworks and effective incident response plans that integrate advanced technologies to reduce breach identification times and mitigate costs (ITRC, 2023).

Literature Review

The research from the Journal of Cybersecurity presents a perspective on how data breaches affect a firm's reputation, contrasting with the often-assumed uniformly negative impact. According to this study, while large and salient data breaches typically result in a 5-9% decline in a company's reputational intangible capital, smaller breaches can increase reputational intangible capital by 26-29%. This variation underscores the nuanced nature of consumer and public responses to data breaches, suggesting that the impact on reputation may depend significantly on the breach's visibility and the company's industry sector. For larger companies in these sectors, a breach is more likely to result in reputational damage, likely due to higher consumer expectations and greater scrutiny (Makridis, 2021).

In the 2018 study "Effect of a Data Breach Announcement on Customer Behavior," Ramkumar Janakiraman, Joon Ho Lim, and Rishika Rishika investigate how announcements of data breaches affect consumer spending and behavior across different retail channels. Utilizing a natural experiment design, they analyze transaction data from a multichannel retailer, contrasting customer behaviors before and after a data breach announcement. The study employs a difference-in-differences analytical framework to discern the impact on two groups: those whose data was compromised and a control group whose data was not affected. This method helps isolate the effect of the breach from other variables, providing a clear picture of its direct impact on customer spending and channel preference.

The findings reveal that data breach announcements lead to a significant reduction in customer spending, with affected customers reducing their expenditure by approximately 32.45% compared to unaffected customers. Additionally, there is a noticeable shift in purchasing behaviors, with customers migrating from compromised channels to those perceived as secure. This migration, however, is less pronounced among customers who exhibit higher levels of loyalty and patronage towards the retailer. These loyal customers show more resilience in their spending habits, suggesting that strong customer relationships can buffer the negative impacts of data breaches (Janakiraman, 2018).

The 2022 study by Hamid Reza Nikkhah and Varun Grover, "An Empirical Investigation of Company Response to Data Breaches," meticulously examines the strategic responses of publicly traded U.S. companies following data breaches and their consequential impacts on crucial stakeholders: customers and investors. The research categorizes these corporate responses into several types including corrective actions, apologies, and compensations, along with observing companies that opt for no action. The findings reveal distinct nuances in how different responses affect stakeholders. Corrective actions alone were less effective compared to strategies that included apologies or compensations in mitigating negative customer reactions. Moreover, while these comprehensive responses, such as apologies and compensations, help to stabilize stock prices, they were significantly more effective when implemented promptly after a breach. This highlights the critical role of response timing, with immediate actions proving more efficacious in assuaging both customer and investor concerns (Nikkhah & Grover, 2022).

The 2020 study by Dennis D. Malliouris and Andrew Simpson, "Underlying and Consequential Costs of Cyber Security Breaches: Changes in Systematic Risk," delves into the financial repercussions of cyber security breaches on publicly listed companies, particularly focusing on the changes in systematic risk. The authors use an event study methodology in conjunction with the Capital Asset Pricing Model (CAPM) to examine the impact on firms' beta values, which measure systematic risk. By evaluating 202 severe security breaches from 2005 to 2019, they explore how these incidents alter the perceived risk of companies through changes in regular, upside, and downside betas, providing a nuanced understanding of the asymmetrical effects of security breaches.

Their methodological approach is meticulous, employing both regular and dual-beta models to assess the different behaviors of stock prices in varying market conditions (bearish vs. bullish). This dual-beta model is particularly insightful as it differentiates the risk exposure during positive and negative market returns, a significant refinement over traditional single-beta analyses. The findings of Malliouris and Simpson reveal that severe cyber breaches significantly elevate the systematic risk of affected firms, evidenced by increased regular and downside betas, whereas upside betas remain unaffected. This indicates that the market perceives a higher risk in these firms, particularly in adverse conditions, leading to increased equity costs. The implications are profound for corporate financial strategy, as higher systematic risk translates into higher costs of capital, potentially influencing investment and operational decisions (Malliouris & Simpson, 2020).

In the 2023 study "Cyber Terrorism Cases and Stock Market Valuation Effects," Katherine Taken Smith, Lawrence Murphy Smith, Marcus Burger, and Erik S. Boyle examine the economic repercussions of cyber terrorism on the stock market values of publicly traded companies. Defining cyber terrorism as digital attacks intended to influence political or social objectives, the research quantifies the adverse effects on firms' market valuations compared to the Dow Jones Index. This analysis is vital, bridging the gap between the cybersecurity breaches and their tangible financial impacts on corporate finance, providing a unique insight into the extent of economic disruption caused by such security incidents. The authors employ an event study methodology, focusing on stock price fluctuations of affected companies around the time of cyber terrorism incidents reported in news stories. They track stock movements 1, 3, and 7 days before and after these incidents and compare them with the Dow Jones Industrial Average to gauge the specific

financial impact. The findings reveal that stock prices of targeted companies significantly decline relative to the market immediately following cyber terrorism incidents, underscoring the swift financial damage and erosion of investor confidence. In all examined post-incident periods, the affected firms' stocks consistently showed a marked negative performance compared to the Dow Jones Index (Smith, 2023).

Methodology

Data collection for this study will be conducted using the methodology outlined in Smith et al (2023) which used financial data 7 days prior and 7 days following a publicly disclosed security breach, and using statistical analysis to determine if the breaches significantly impacted the change in stock price by comparing the stock price to the performance of the Dow Jones Industrial Average (DJIA).. The data was downloaded from Yahoo Finance, a reliable source of historical financial information for publicly traded companies. The metrics collected include daily stock prices and Earnings Per Share (EPS), both crucial indicators of a company's financial health and market performance.

The sample consists of publicly traded companies that have experienced a cybersecurity breach with a publicly disclosed date. The inclusion criteria ensure that the impact of the breach on stock prices can be directly associated with the event. For each disclosure date, stock data will be collected for a specified event window, typically 7 days before and 7 days after the breach disclosure. This data includes the stock's open price, close price, and volume, as well as the DJIA open price, close price, and volume, providing a comprehensive view of market activity in the context of the cybersecurity event.

To determine the significance of abnormal returns following cybersecurity incidents, rigorous statistical testing will be employed. The matched-pair t-test, suitable for paired observations of market and event returns, will evaluate whether breaches significantly impact stock prices by comparing average abnormal returns during the event window to a theoretical mean of zero. This test calculates the difference between these paired observations and assesses whether the mean of these differences is significantly different from zero. The t-statistic measures the size of the difference relative to the variation in the sample data, and a significant t-statistic indicates that the breach had a statistically significant impact on stock prices.

In addition to the matched-pair t-test, the Wilcoxon signed-rank test will be used to reinforce the findings. This non-parametric test ranks the differences between paired observations and evaluates whether the median difference is significantly different from zero. The Wilcoxon test is useful when the data does not meet the normality assumption required by the paired t-test, providing a robust analysis of abnormal returns. The Pearson correlation tests will examine the linear relationship between stock price changes and broader market movements, such as the DJIA. This test calculates the correlation coefficient, indicating the strength and direction of the linear relationship between two variables. When linear relationships are insufficient, the Mann-Whitney U test will compare distributions of abnormal and market returns by ranking all observations and evaluating the differences in ranks between the two samples. This non-parametric test is particularly useful for detecting significant differences when the data is not normally distributed.

Limitations

One significant limitation of this study is its reliance on publicly available financial data, which may not capture all relevant variables influencing stock price movements. While the data includes stock prices, volumes, and broader market indices, it does not account for other influential factors such as investor sentiment, media coverage, or concurrent economic events that could also impact stock prices. Additionally, the study's focus on a specific window around the breach disclosure date may overlook longer-term effects

or delayed market reactions, potentially leading to an incomplete understanding of the breach's full impact on stock prices. Another limitation is the inherent variability in the nature and scale of the cybersecurity breaches studied. Each breach differs in scope, the sensitivity of the data compromised, and the company's response, which can lead to varying degrees of market reaction and make it challenging to generalize the findings across all types of cybersecurity incidents. Furthermore, the use of multiple statistical tests, while comprehensive, may introduce complexity that could be difficult for non-quantitative readers to interpret.

Case Studies

Capital One

The 2019 Capital One data breach was a significant security incident where an individual exploited a misconfiguration in Capital One's Amazon Web Services (AWS) infrastructure. This breach resulted in unauthorized access to the personal information of approximately 106 million individuals in the United States and Canada. The attacker, Paige Thompson, was able to extract sensitive data including names, addresses, zip codes, phone numbers, email addresses, dates of birth, and self-reported income, as well as about 140,000 Social Security numbers and 80,000 linked bank account numbers of secured credit card customers from the U.S., and approximately 1 million Social Insurance Numbers from Canadian customers. The vulnerability was in a misconfigured web application firewall that allowed the attacker to execute commands and exfiltrate data (Seals, 2022).

Equifax

In 2017, the Equifax data breach emerged as one of the most significant cybersecurity events, impacting approximately 145 million Americans. Orchestrated by hackers affiliated with the Chinese military, the breach exploited a vulnerability in Equifax's dispute resolution website. Once inside the system, the attackers employed several sophisticated techniques to access and extract sensitive data, including Social Security numbers, birthdates, and addresses. This breach highlighted critical lapses in Equifax's security posture, particularly in patch management and intrusion detection, which failed to prevent or detect unauthorized access promptly (Federal Trade Commission, 2019).

Facebook

This breach was initially identified by Facebook on September 25, 2018, after a spike in unusual activity was detected on September 14, affecting up to 50 million users, was a significant security incident where attackers exploited a vulnerability in the platform's "View As" feature. This vulnerability allowed attackers to steal Facebook access tokens, which could be used to take over people's accounts. These tokens are digital keys that keep users logged in to Facebook, so they don't need to re-enter their password each time they use the app. Facebook responded by fixing the vulnerability, resetting the access tokens of the approximately 90 million accounts that were potentially affected to protect user security, and temporarily turning off the "View As" feature (Frenkel & Isaac, 2018).

The Facebook data breach disclosed on April 3, 2021, involved the unauthorized access of personal data belonging to approximately 533 million users worldwide. The breach resulted from the exploitation of a vulnerability in Facebook’s contact importer feature, which allowed attackers to scrape users’ personal information, including names, phone numbers, email addresses, and other profile details. Although Facebook reported that the data was old and had been obtained through previous vulnerabilities patched in 2019, the large scale of the exposure reignited concerns about Facebook’s ability to safeguard user

information (Bowman, 2021).

JBS S.A.

In May 2021, JBS S.A., one of the world's largest meat processing companies, suffered a severe ransomware attack executed by the notorious REvil group, also known as Sodinokibi. This cybercriminal group, operating primarily out of Eastern Europe, exploited vulnerabilities in JBS's cybersecurity to deploy ransomware across JBS's North American and Australian IT systems. The disruption forced JBS to shut down several of its operations, significantly impacting its ability to process meat and threatening parts of the global food supply chain. The initial intrusion vector for the attack is believed to have been through a compromised Remote Desktop Protocol (RDP) or possibly using previously leaked employee credentials found on the dark web. Once access was gained, the attackers deployed ransomware, which encrypted data across JBS's affected networks, rendering them inoperable (Sherstobitoff, 2021).

MGM Resorts International

The 2020 data breach at MGM Resorts International involved the personal information of approximately 10.6 million guests, which included sensitive data such as names, addresses, phone numbers, email addresses, and birth dates. This information was posted on a hacking forum, revealing the data of many high-profile individuals, including celebrities, CEOs, and government officials. The breach, discovered in the summer of 2019, did not include the leakage of financial details like credit card numbers or passwords. MGM Resorts had identified the breach upon discovering unauthorized access to a cloud server containing this guest information. Following the breach, MGM undertook significant steps to notify affected individuals and strengthen their security measures to prevent future incidents. The leaked data notably included guests who stayed at MGM properties no later than 2017 (Cimpanu, 2020).

Nvidia

In March 2022, Nvidia experienced a significant cybersecurity breach orchestrated by the Lapsus$ hacking group, which resulted in the theft and subsequent leak of sensitive data from over 71,000 employees. The stolen data included not only employee credentials but also proprietary Nvidia information such as source code for Nvidia’s hash rate limiter, which impacts the Ethereum mining performance of its RTX 30-series graphics cards. The hackers threatened to release more stolen data unless Nvidia removed certain software limitations from their products. Despite the severity of the breach, Nvidia assured customers that it did not expect any disruption to its business operations or its ability to serve customers. The company immediately took steps to secure its systems, involving law enforcement and cybersecurity experts to mitigate the breach's effects (Hope, 2022).

Okta

The 2022 Okta data breach, orchestrated by the cybercriminal group Lapsus$, primarily involved unauthorized access to a subcontractor's systems that potentially affected hundreds of clients. This breach highlighted significant vulnerabilities within Okta's security protocols, particularly concerning third-party vendor management. The attackers gained control over a workstation used by a support engineer from the subcontractor Sitel, gaining access for a brief 25-minute window on January 21, 2022. During this period, they accessed two active customer tenants and viewed limited additional information in applications such as Slack and Jira. Despite the short duration of access, the breach was significant due to the sensitive nature of the data involved and the potential for wider exploitation across Okta's extensive customer base (Bradbury, 2022).

SolarWinds

The SolarWinds cyberattack of 2020, known as the SUNBURST backdoor, represents one of the most sophisticated and far-reaching cybersecurity breaches in history. Initiated by a group linked to the Russian Foreign Intelligence Service, the attackers implanted malicious code into the SolarWinds Orion platform, which is extensively utilized across various sectors for network management. This code functioned as a backdoor for further intrusions, affecting an estimated 18,000 organizations, including major U.S. government agencies and technology companies such as Microsoft and Cisco (Oladimeji & Kerner, 2023).

T-Mobile

The first major T-Mobile data breach in 2023, disclosed on January 19, 2023, affected approximately 37 million customers, marking another significant security incident for the company. This breach involved unauthorized access through an API starting around November 25, 2022, allowing extensive extraction of customer data, including names, billing addresses, email addresses, phone numbers, dates of birth, account numbers, and plan details. Despite the vast scale of the breach, T-Mobile confirmed that Social Security numbers, passwords, and financial details were not compromised, limiting the potential for direct financial fraud but still posing significant risks for identity theft and unauthorized account access (Krebs on Security, 2023).

The second major T-Mobile data breach in 2023, disclosed on April 28, impacted fewer than 1,000 customers but involved sensitive data including Social Security numbers, ID numbers, and account PINs. This breach, though smaller in scale compared to the January incident affecting 37 million accounts, highlighted significant vulnerabilities as it involved critical personal and security data, which could lead to severe risks of identity theft and fraud for those affected. This breach was again attributed to unauthorized access, this time through a different set of compromised credentials that were not connected to the earlier incident in January. T-Mobile responded quickly by identifying and blocking malicious access, notifying impacted customers, and offering comprehensive credit monitoring and identity theft protection services to those affected (Blair-Frasier, 2023).

Results

To set up the results for readers unfamiliar with quantitative studies, it's essential to explain the statistical tests used and their significance. A paired t-test was conducted for each company to assess the impact of cybersecurity breaches on stock prices by comparing prices before and after the breach for statistical significance. The Wilcoxon signed-rank test, a non-parametric alternative, was used to verify the results by evaluating median differences. The Pearson correlation test examined the linear relationship between stock price changes and broader market movements. Finally, the Mann-Whitney U test compared distributions of abnormal and market returns, useful for detecting significant differences in non-normally distributed data.

Capital One

The paired t-test produced a statistic of -5.6374 with a p-value of 0.0003, indicating a statistically significant difference between Capital One's stock price changes and Dow Jones changes. This suggests that the breach had a substantial impact on Capital One's stock prices. Similarly, the Wilcoxon signed-rank test confirmed this significance with a statistic of 3.0000 and a p-value of 0.0098, reinforcing the breach's impact. The

Pearson correlation test, which yielded a coefficient of 0.5078 and a p-value of 0.1340, suggested no significant linear relationship between stock price changes and broader market movements. This implies that the influence of the breach does not follow a straightforward linear pattern. The Mann-Whitney U test indicated a statistically significant difference with a statistic of 20.0 and a p-value of 0.0257, further supporting the breach's impact. Additionally, the analysis revealed a stock price volatility standard deviation of 1.5437, compared to a Dow Jones volatility standard deviation of 1633.04. The average stock volume was approximately 4,090,470 shares, while the average Dow Jones volume was about 287,863,000 shares. These comprehensive statistical analyses confirm the significant financial repercussions of the Capital One cybersecurity breach on its stock prices.

Table 1: Capital One

Test	Statistic	P-value	Significance
Paired t-test	-5.6374	0.0003	**Statistically significant**
Wilcoxon signed-rank test	3	0.0098	**Statistically significant**
Pearson correlation test	0.5078	0.134	Not significant
Mann-Whitney U test	20	0.0257	**Statistically significant**

Equifax

The paired t-test showed a t-statistic of -130.0955 and a p-value of less than 0.0001, indicating a statistically significant difference between stock price changes and DJIA changes. This result suggests that the Equifax breach had a profound impact on stock prices. The Wilcoxon signed-rank test confirmed this significance with a statistic of 0.0 and a p-value of 0.0039. However, the Pearson correlation test indicated no significant linear relationship, with a coefficient of -0.4527 and a p-value of 0.2211. This implies that the influence of the breach does not follow a straightforward linear pattern. The Mann-Whitney U test also showed a significant difference with a statistic of 0.0 and a p-value of 0.0004, further supporting the breach's impact. The analysis revealed a stock price volatility standard deviation of 6.5509, compared to 81.5289 for the DJIA. The average stock volume was approximately 5.93 million shares, while the average DJIA volume was about 319.68 million shares. These comprehensive statistical analyses confirm the significant financial repercussions of the Equifax cybersecurity breach on its stock prices.

Table 2: Equifax

Test	Statistic	P-value	Significance
Paired t-test	-130.0955	< 0.0001	**Statistically significant**
Wilcoxon signed-rank test	0	0.0039	**Statistically significant**
Pearson correlation test	-0.4527	0.2211	Not significant
Mann-Whitney U test	0	0.0004	**Statistically significant**

Facebook

The paired t-test yielded a statistic of -63.6382 with a p-value of 0.0, indicating a statistically significant difference between stock price changes and Dow Jones changes, suggesting that the Facebook breach had a substantial impact on stock prices. Similarly, the Wilcoxon signed-rank test produced a significant result

with a statistic of 0.0 and a p-value of 0.0020, reinforcing the breach's impact. However, the Pearson correlation test resulted in a coefficient of -0.0121 and a p-value of 0.9735, suggesting no significant linear relationship between stock price changes and Dow Jones changes. This implies that the influence of the breach does not follow a straightforward linear pattern. The Mann-Whitney U test indicated a statistically significant difference with a statistic of 0.0 and a p-value of 0.0002, further supporting the breach's impact. Insights showed a stock price volatility standard deviation of 3.0409, compared to a Dow Jones volatility standard deviation of 177.245. The average stock volume was approximately 29,091,300 shares, while the average Dow Jones volume was about 296,592,000 shares. These comprehensive statistical analyses confirm the significant financial repercussions of the Facebook cybersecurity breach on its stock prices.

Table 3: Facebook

Test	Statistic	P-value	Significance
Paired t-test	-63.6382	0	**Statistically significant**
Wilcoxon signed-rank test	0	0.002	**Statistically significant**
Pearson correlation test	-0.0121	0.9735	Not significant
Mann-Whitney U test	0	0.0002	**Statistically significant**

For the breach disclosed on April 5, 2021, the analysis shows a paired t-test statistic of -53.1723 with a p-value of 0.0, indicating a statistically significant difference between stock price changes and Dow Jones changes. The Wilcoxon signed-rank test produced significant results with a statistic of 0.0 and a p-value of 0.0039. The Pearson correlation test resulted in a coefficient of 0.0037 and a p-value of 0.9926, suggesting no significant linear relationship between stock price changes and Dow Jones changes. The Mann-Whitney U test indicated a statistically significant difference with a statistic of 0.0 and a p-value of 0.0004. The insights revealed a stock price volatility standard deviation of 4.0086 and a Dow Jones volatility standard deviation of 507.318. The average stock volume was approximately 20,179,700 shares, while the average Dow Jones volume was about 327,279,000 shares. The analysis for Facebook, Inc. underscores the significant impact of breaches on the company's stock prices. Statistically significant differences were found for all t-tests and Wilcoxon tests across the disclosed dates. The average t-test statistic was -79.2626, and the average correlation coefficient was 0.0137.

Table 4: Facebook

Test	Statistic	P-value	Significance
Paired t-test	-53.1723	0	**Statistically significant**
Wilcoxon signed-rank test	0	0.0039	**Statistically significant**
Pearson correlation test	0.0037	0.9926	Not significant
Mann-Whitney U test	0	0.0004	**Statistically significant**

JBS S.A.

The analysis of the JBS S.A. breach, disclosed on Memorial Day, May 31, 2021, offers critical insights into the company's stock prices in comparison to the DJIA from the next market opening on June 1, 2021. The

paired t-test revealed a significant difference with a statistic of -247.3386 and a p-value of 7.99243E-17, indicating a substantial impact of the breach on JBS's stock prices. This finding was corroborated by the Wilcoxon signed-rank test, which also showed a significant difference with a statistic of 0.0 and a p-value of 0.0039. Conversely, the Pearson correlation test indicated no significant linear relationship, with a coefficient of 0.0468 and a p-value of 0.9048, suggesting that the breach's influence does not follow a simple linear pattern. The Mann-Whitney U test further supported the significant difference, yielding a statistic of 0.0 and a p-value of 0.0004. The analysis highlighted a stock price volatility standard deviation of 0.1952, compared to a Dow Jones volatility standard deviation of 112.863. The average stock volume was approximately 138,556 shares, while the average DJIA volume was about 305.77 million shares. These comprehensive statistical analyses confirm the significant financial impact of the JBS S.A. cybersecurity breach on its stock prices.

Table 5: JBS S.A.

Test	Statistic	P-value	Significance
Paired t-test	-247.3386	7.99E-17	**Statistically significant**
Wilcoxon signed-rank test	0	0.0039	**Statistically significant**
Pearson correlation test	0.0468	0.9048	Not significant
Mann-Whitney U test	0	0.0004	**Statistically significant**

MGM Resorts International

The paired t-test yielded a statistic of -30.5767 with a p-value of 2.09569E-10, indicating a statistically significant difference between MGM Resorts International's stock price changes and Dow Jones changes. Similarly, the Wilcoxon signed-rank test confirmed this significance with a statistic of 0.0000 and a p-value of 0.001953. The Pearson correlation test resulted in a coefficient of 0.6982 and a p-value of 0.0247, suggesting a significant positive linear relationship between stock price changes and Dow Jones changes. The Mann-Whitney U test further supported these findings, showing a statistically significant difference with a statistic of 0.0 and a p-value of 0.0002. Additional insights revealed a stock price volatility standard deviation of 0.7698 and a Dow Jones volatility standard deviation of 498.818. The average stock volume was approximately 11,353,770 shares, compared to the average Dow Jones volume of about 375,615,000 shares. These comprehensive analyses from both the t-test and Wilcoxon test confirm that there are statistically significant differences between MGM Resorts International's stock price changes and broader market movements as measured by the DJIA.

Table 6: MGM Resorts

Test	Statistic	P-value	Significance
Paired t-test	-30.5767	2.10E-10	**Statistically significant**
Wilcoxon signed-rank test	0	0.001953	**Statistically significant**
Pearson correlation test	0.6982	0.0247	**Statistically significant**
Mann-Whitney U test	0	0.0002	**Statistically significant**

Nvidia

A paired t-test yielded a statistic of -45.5502 with a p-value of 0.0000, indicating a statistically significant difference between Nvidia's stock price changes and those of the DJIA. The Wilcoxon signed-rank test also confirmed this significance, with a statistic of 0.0 and a p-value of 0.0039. The Pearson correlation test revealed a coefficient of 0.6830 and a p-value of 0.0426, suggesting a significant positive linear relationship between Nvidia's stock price changes and DJIA changes. The Mann-Whitney U test further supported the presence of a significant difference, with a statistic of 0.0 and a p-value of 0.0004. Additional analysis indicated a stock price volatility standard deviation of 12.7363 for Nvidia, compared to 675.799 for the DJIA. The average stock volume for Nvidia was approximately 62,872,200 shares, while the average DJIA volume was about 422,064,000 shares.

Table 7: Nvidia

Test	Statistic	P-value	Significance
Paired t-test	-45.5502	0.0	Statistically significant
Wilcoxon signed-rank test	0	0.0039	Statistically significant
Pearson correlation test	0.683	0.0426	Statistically significant
Mann-Whitney U test	0	0.0004	Statistically significant

Okta

The paired t-test showed a significant difference in stock price changes for Okta, with a t-statistic of -73.5111 and a p-value of 0.0, indicating that the breach had a substantial impact on stock prices compared to the DJIA. Similarly, the Wilcoxon signed-rank test confirmed this finding, showing a statistically significant difference with a statistic of 0.0 and a p-value of 0.0020. The Pearson correlation test, however, revealed no significant linear relationship between Okta's stock price changes and the DJIA, with a coefficient of 0.1465 and a p-value of 0.6862. This suggests that while the breach significantly affected Okta's stock prices, this impact did not follow a simple linear pattern in relation to broader market movements. Additionally, the Mann-Whitney U test further confirmed the significant difference in stock price changes, with a statistic of 0.0 and a p-value of 0.0002. The analysis also highlighted a stock price volatility standard deviation of 8.4045 for Okta, compared to 466.064 for the DJIA, with average stock volumes of approximately 4,803,430 shares for Okta and 383,379,000 shares for the DJIA. These findings underscore the significant impact of the Okta data breach on its stock prices, independent of broader market trends.

Table 8: Okta

Test	Statistic	P-value	Significance
Paired t-test	-73.5111	0.0	Statistically significant
Wilcoxon signed-rank test	0	0.002	Statistically significant
Pearson correlation test	0.1465	0.6862	Not significant
Mann-Whitney U test	0	0.0002	Statistically significant

SolarWinds

The paired t-test yielded a statistic of -94.8321 with a p-value of 0.0, indicating a significant difference between stock price changes and DJIA changes, underscoring the impact of the SolarWinds breach. The Wilcoxon signed-rank test also confirmed this significance with a statistic of 0.0000 and a p-value of 0.002. Conversely, the Pearson correlation test resulted in a coefficient of -0.1525 and a p-value of 0.6741, suggesting no significant linear relationship between stock price changes and the broader market movements. The Mann-Whitney U test further supported the significant difference with a statistic of 0.0 and a p-value of 0.0002. Additional analysis revealed that the stock price volatility standard deviation for SolarWinds was 1.236, compared to the DJIA's volatility standard deviation of 278.528. The average stock volume for SolarWinds was approximately 2,654,420 shares, while the average DJIA volume was about 407,685,000 shares. These results collectively highlight the substantial impact of the SolarWinds cyberattack on its stock performance.

Table 9: SolarWinds

Test	Statistic	P-value	Significance
Paired t-test	-94.8321	0.0	Statistically significant
Wilcoxon signed-rank test	0	0.002	Statistically significant
Pearson correlation test	-0.1525	0.6741	Not significant
Mann-Whitney U test	0	0.0002	Statistically significant

T-Mobile

The paired t-test yielded a highly significant t-statistic of -144.8332 with a p-value of 0.0, indicating a substantial difference in T-Mobile's stock price changes compared to the DJIA. This finding is supported by the Wilcoxon signed-rank test, which resulted in a Wilcoxon statistic of 0.0000 and a p-value of 0.002, further confirming notable disparities in stock price movements. In contrast, the Pearson correlation test produced a coefficient of 0.2892 with a p-value of 0.4177, suggesting no significant linear relationship between T-Mobile's stock price changes and those of the DJIA. Additional analysis revealed that T-Mobile's stock price volatility was 0.6309, compared to the DJIA's volatility of 233.839. During this period, the average stock volume for T-Mobile was approximately 3,789,970 shares, while the average DJIA volume was about 267,079,000 shares.

Table 10: T-Mobile

Test	Statistic	P-value	Significance
Paired t-test	-144.8332	0.0	**Statistically significant**
Wilcoxon signed-rank test	0	0.002	**Statistically significant**
Pearson correlation test	0.2892	0.4177	Not significant
Mann-Whitney U test	0	0.0002	**Statistically significant**

The paired t-test revealed a highly significant t-statistic of -35.1890 with a p-value of 0.0, indicating a substantial difference between T-Mobile's stock price changes and those of the DJIA. This result was further supported by the Wilcoxon signed-rank test, which produced a Wilcoxon statistic of 0.0 and a p-value of 0.0039, reaffirming the significant impact. Conversely, the Pearson correlation analysis showed a coefficient of 0.4213 with a p-value of 0.2587, indicating no significant linear relationship between T-Mobile's stock price changes and the DJIA. Additional insights revealed that T-Mobile's stock price volatility was 1.7647, compared to the DJIA's volatility of 550.689. The average stock volume for T-Mobile during this period was approximately 5,063,680 shares, while the average DJIA volume was about 332,297,000 shares.

Table 11: T-Mobile

Test	Statistic	P-value	Significance
Paired t-test	-35.189	0.0	**Statistically significant**
Wilcoxon signed-rank test	0	0.0039	**Statistically significant**
Pearson correlation test	0.4213	0.2587	Not significant
Mann-Whitney U test	0	0.0002	**Statistically significant**

Both T-Mobile breaches in 2023 had a significant impact on the company's stock prices, as indicated by the paired t-test and Wilcoxon signed-rank test results. The first breach, disclosed in January 2023, affected approximately 37 million customers and demonstrated a substantial deviation in T-Mobile's stock price changes compared to the DJIA, with a t-statistic of -144.8332 and a p-value of 0.0. Similarly, the second breach in April 2023, involving sensitive data of fewer than 1,000 customers, showed significant stock price differences with a t-statistic of -35.1890 and a p-value of 0.0. The Wilcoxon signed-rank tests further confirmed these findings with statistically significant results. However, the Pearson correlation tests suggested no significant linear relationship between T-Mobile's stock price changes and those of the DJIA for both breaches, indicating that the market reactions to these breaches do not follow a simple linear pattern.

Discussion

The findings from the analysis of various cybersecurity breaches provide a comprehensive understanding of the financial repercussions that these incidents can have on the stock prices of affected companies. The paired t-test results consistently showed statistically significant differences in stock price changes before and after the breaches, indicating substantial impacts on the market valuation of the companies studied. For instance, the breaches at Capital One, Equifax, and Facebook all resulted in significant deviations from their respective market indices, as evidenced by their paired t-test statistics and corresponding p-values.

Interestingly, the Wilcoxon signed-rank tests corroborated the findings of the paired t-tests, further reinforcing the significance of the breaches on stock prices. This non-parametric test provided additional validation of the observed impacts, particularly for companies like JBS S.A. and MGM Resorts International, which also demonstrated significant changes in stock prices post-breach. The consistency between these two tests across multiple cases strengthens the argument that cybersecurity breaches have a profound and measurable effect on stock market performance. However, the Pearson correlation tests often did not show significant linear relationships between stock price changes and broader market movements, suggesting that the market reactions to these breaches do not follow a straightforward linear pattern. This

highlights the complexity of market responses to cybersecurity incidents, influenced by various factors beyond the immediate financial data.

Furthermore, the Mann-Whitney U test results provided additional insights into the distributional differences in stock price changes, confirming significant disparities in several cases. This test was particularly useful in highlighting the non-normally distributed nature of the data, reinforcing the robustness of the findings. The volatility analysis revealed that stock price fluctuations increased markedly following breaches, as seen in companies like Nvidia and T-Mobile. This increased volatility reflects heightened investor uncertainty and potential long-term repercussions on company valuation and investor confidence.

Contributions

This study makes several key contributions to the understanding of the financial impacts of cybersecurity breaches on publicly traded companies. Firstly, it provides empirical evidence demonstrating the significant negative effects of data breaches on stock prices, highlighting the urgent need for robust cybersecurity measures in corporate governance. By employing rigorous statistical methods, including matched-pair t-tests and Wilcoxon signed-rank tests, the study isolates the specific financial repercussions of breaches, offering a clear quantification of market reactions. Secondly, the research offers a nuanced view of reputational impacts, showing that while large breaches typically harm reputations, smaller breaches can sometimes enhance a company's perceived trustworthiness.

Future Research

Future research should explore the evolving landscape of cybersecurity threats and their financial impacts on different sectors. While this study has provided significant insights into the financial repercussions of data breaches on publicly traded companies, there is a need to delve deeper into sector-specific analyses. For instance, future studies could focus on comparing the financial impacts across various industries such as healthcare, finance, and technology, examining how regulatory environments and industry-specific security measures influence the outcomes of breaches. Additionally, there is a growing need to understand the long-term effects of repeated breaches on a company's financial health and market performance.

Conclusion

The substantial financial impact of cybersecurity breaches on publicly traded companies is evident from the consistent statistical significance observed across various case studies. For instance, the Capital One breach demonstrated a significant deviation in stock price changes with a paired t-test statistic of -5.6374 and a p-value of 0.0003, while Equifax's breach analysis revealed a paired t-test statistic of -130.0955 and a p-value of less than 0.0001. Similarly, the Facebook breaches showed t-test statistics of -63.6382 and -53.1723, both with p-values of 0.0, indicating significant deviations compared to the DJIA. The Wilcoxon signed-rank test and the Mann-Whitney U test consistently confirmed significant differences, reinforcing the market's sensitivity to these incidents. However, the Pearson correlation test often did not show a significant linear relationship, suggesting that the market's reaction to cybersecurity breaches is influenced by various factors beyond straightforward linear patterns.

These findings highlight the critical need for robust cybersecurity measures and proactive incident response strategies. The financial markets' response to breaches underscores the importance of not only preventing such incidents but also managing their aftermath effectively. Companies must invest in advanced security technologies and develop comprehensive breach response plans to mitigate potential financial losses.

Addressing investor sentiment and public perception through transparent communication and effective crisis management can help mitigate the adverse effects on stock prices and investor confidence. By understanding the multifaceted impacts of cybersecurity breaches and investing in comprehensive security measures, companies can better protect their financial stability and market reputation.

References

Blair-Frasier, R. (2023, May 4). *T-Mobile confirms second data breach in 2023*. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/99300-t-mobile-confirms-second-data-breach-in-2023

Bowman, E. (2021, April 9). *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*. Retrieved from NPR: https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Bradbury, D. (2022, April 19). *Okta Concludes its Investigation Into the January 2022 Compromise*. Retrieved from Okta: https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/

Cimpanu, C. (2020, February 19). *Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum*. Retrieved from ZDNet: https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/

Federal Trade Commission. (2019, June 22). *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*. Retrieved from Federal Trade Commission: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

Frenkel, S., & Isaac, M. (2018, Septemeber 28). *Facebook Security Breach Exposes Accounts of 50 Million Users*. Retrieved from New York Times: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

Hope, A. (2022, March 11). *Nvidia Data Leak Exposed Proprietary Information but Wasn't a Russian Ransomware Attack, Company Says*. Retrieved from CPO Magazine: https://www.cpomagazine.com/cyber-security/nvidia-data-leak-exposed-proprietary-information-but-wasnt-a-russian-ransomware-attack-company-says/

ITRC. (2023). *Annual Data Breach Report.* Retrieved from Identity Theft Resource Center (ITRC): https://www.idtheftcenter.org/publication/2023-data-breach-report/

Janakiraman, R. L. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing*, 85-105.

Krebs on Security. (2023, January 19). *New T-Mobile Breach Affects 37 Million Accounts*. Retrieved from Krebs on Security: https://krebsonsecurity.com/2023/01/new-t-mobile-breach-affects-37-million-accounts/

Makridis, C. A. (2021, September). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*.

Malliouris, D., & Simpson, A. (2020). Underlying and consequential costs of cyber security breaches: Changes in systematic risk. *Workshop on the Economics of Information Security*.

Nikkhah, H., & Grover, V. (2022). An Empirical Investigation of Company Response to Data Breaches. *MIS Quarterly*, An Empirical Investigation of Company Response to Data Breaches.

Oladimeji, S., & Kerner, S. M. (2023, November 3). *SolarWinds hack explained: Everything you need to know*. Retrieved from TechTarget: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Proofpoint. (2023). *What Is a Data Breach?* Retrieved from Proofpoint: https://www.proofpoint.com/us/threat-reference/data-breach

Seals, T. (2022, June 20). *Capital One Attacker Exploited Misconfigured AWS Databases*. Retrieved from Dark Reading: https://www.darkreading.com/cyberattacks-data-breaches/capital-one-attacker-exploited-misconfigured-aws-databases

Sherstobitoff, R. (2021, June 8). *JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified*. Retrieved from SecurityScorecard: https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march/

Smith, K. T. (2023). Cyber terrorism cases and stock market valuation effect. *Information & Computer Security*, 385-403.