Cybersecurity Events, Financial Analysts, and Earnings Forecast Uncertainty

Long Thanh Bui

A Thesis

In the Department of Accountancy at

John Molson School of Business

Presented in Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy in Administration (Accountancy) at

Concordia University

Montreal, Quebec, Canada

November 2023

CONCORDIA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: Long Thanh Bui

Entitled: Cybersecurity Events, Financial Analysts, and Earnings Forecast Uncertainty

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

Doctor Of Philosophy Business Administration (Accountancy)

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. Saif Ullah

____External Examiner

Dr. Bruce McConomy

____Examiner

Dr. Luo He

____Examiner

Dr. Eduardo Schiehll

____Thesis Supervisors

Dr. Michel Magnan and Dr. Rucsandra Moldovan

Approved by

____

Dr. Tracy Hetch, Graduate Program Director

11 October, 2023

____

Dr. Anne-Marie Croteau, Dean of Faculty

Abstract

Cybersecurity Events, Financial Analysts, and Earnings Forecast Uncertainty

Long Thanh Bui, PhD

Concordia University, 2023

This dissertation examines the role of financial analysts in evaluating cybersecurity events within the commercial banking industry. The focus on commercial banks arises from their visibility and attractiveness as cyber attack targets. The increasing number of such incidents in recent years has garnered significant public scrutiny, especially from investors and analysts. The situation engenders a sense of ambiguity regarding the outlook of the affected business.

The dissertation comprises two complementary empirical chapters. Chapter 2 presents an exploratory case study on financial analysts' interactions with management in the context of conference calls following cyber incidents. Such interaction provides insights into the kind of information that financial analysts seek from management, and which presumably enters analysts' decision-making process when forecasting a bank's financial situation. The case study reveals that financial analysts ask more questions about cyber-related issues such as digital fraud, cloud technology, and technological investments to encourage top management at some banks to discuss their prevention efforts concerning cybersecurity risks and controls. When asked directly, managers discuss cyber incidents upfront.

Chapter 3 examines how cybersecurity incidents at commercial banks affect analyst forecast properties. Cyber incidents affect financial analysts' information environment on two dimensions: uncertainty and information asymmetry. After security breaches, information asymmetry increases due to management's standard practice of securing cybersecurity data to mitigate potential negative financial consequences. Despite the high information asymmetry underlying their earnings forecasts, analysts seek to improve the information environment's quality and reduce uncertainty in the financial market.

Financial analysts who change their earnings forecasts in reaction to cyber attacks do not necessarily do better than those who did not revise their forecasts. Prior studies show that low information asymmetry reduces forecasting risks and drives financial analysts to revise earnings forecasts regularly. Since cyber information is scarce, financial analysts are reluctant to change their earnings estimates when information asymmetry is high. In addition, analysts exhibit different forecasting behaviors depending upon the type of cyber event (involving confidentiality, integrity or availability issues).

This thesis provides new insight into the information dynamics around cybersecurity by concentrating on a significant market intermediary. The thesis contributes to the literature on financial analysts by highlighting their demand for information related to cybersecurity issues and reactions to cybersecurity events. Thus, this thesis advances our understanding of the inputs analysts use in decision-making and how they respond to events that exacerbate uncertainty and information asymmetry in the information environment. Regulators could use these findings to orient their policies regarding mandatory disclosure requirements or guidance on cybersecurity issues. Managers can learn about what cybersecurity-related disclosures capital markets require.

Acknowledgements

I would like to convey my profound appreciation to my esteemed supervisors, Dr. Michel Magnan and Dr. Rucsandra Moldovan, for their excellent guidance, unwavering support, and constructive comments. I express my gratitude to my supervisors for their encouragement despite the considerable challenges I have faced during the Covid-19 pandemic. Furthermore, the successful completion of this endeavor would not have been possible without the invaluable contributions of my defense committee, whose extensive knowledge and expertise were graciously shared. Furthermore, the successful execution of this undertaking would not have been feasible without the crucial support provided by the Luc Beauregard Centre, which generously sponsored the purchase of the Advisen database.

It would be negligent of me to omit acknowledgment of my family, particularly with regards to my parents, my brother and my fiancée. The unwavering faith that others have placed in my abilities has been a source of motivation throughout this endeavor.

Table of Contents
CHAPTERS

1. Introduction

Concerns about data breaches and the ability to pursue operations following a cyber breach underlie the current rise in cybersecurity investments by organizations worldwide. For example, following the Equifax and Anthem data breaches, several United States (U.S.) companies raised their cybersecurity investments to improve their Information Technology (IT) critical infrastructure and reduce cyber vulnerabilities.[1] However, at the same time, many businesses, including banks, are investing in digital technology to enhance their service offerings to customers and to raise their productivity, thus potentially increasing their cyber risk levels. As the level of uncertainty about cyber risk increases, the need to foster investor confidence leads many firms to enhance their disclosure surrounding cybersecurity and cyber risk management (Havakhor et *al.*, 2020).

Cybersecurity aims to safeguard private digital information by restricting its access only to legitimate employees or customers while maintaining the effectiveness and efficiency of that information (Gordon et al., 2006). However, the cybersecurity requirements and what constitutes a cybersecurity incident are subject to different levels of regulations. For instance, U.S. bank branches in European countries must conform to the European Union General Data Protection Act. In contrast, bank branches in New York must follow the New York Cyber Regulation.[2] All banks licensed or registered in New York must comply with the New York Cyber Regulation by updating

[1] Bank of America raised more than $1 billion cybersecurity investments per year (https://www.cnbc.com/2021/06/14/bank-of-america-spends-over-1-billion-per-year-on-cybersecurity.html)
JP Morgan raised almost $600 million cybersecurity investment per year (https://www.nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html)
After having a discussion with United States president Biden, both Microsoft and Google are going to raise $4 billion and $2 billion per year respectively from now until 2027. (https://www.cnbc.com/2021/08/25/google-microsoft-plan-to-spend-billions-on-cybersecurity-after-meeting-with-biden.html?&qsearchterm=cybersecuirty%20spending)

[2] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
https://www.dfs.ny.gov/industry_guidance/cybersecurity

their cybersecurity disclosure annually to the New York Department of Financial Services (Leung, 2018).

Our focus on banks rests on the case that banks possess much client-sensitive information and intellectual properties that link to other industries, thus making them a primary target for hackers. For instance, according to the report by the Identity Theft Resource Center (2018), Banking/Credit/Financial ranked third in the number of records exposed among all sectors.

This dissertation investigates how sell-side financial analysts demand information about cybersecurity incidents in U.S. banks and then incorporate it into their decision-making. The choice of sell-side analysts, rather than buy-side or investment banking analysts, rests on the availability of data about their forecasts on the Institutional Brokers' Estimate System (IBES) database. The focus is how analysts, who possess comprehensive knowledge of the banks' cybersecurity measures through their interaction with top management during conference calls, use this information when a cyber incident occurs. The thesis addresses two main research questions:

RQ1: What information do managers provide about cybersecurity in conference calls, and what information do financial analysts demand?

RQ2: How do financial analysts incorporate cyber-related information in decision-making for their forecasts?

1.1. Goals of the dissertation

Chapter 2 provides an analysis of the Questions and Answers (Q&A) sessions that take place within the quarterly earnings conference calls of five large credit institutions (Bank of America, Bank of New York Mellon, JP Morgan Chase, Citigroup, and Capital One) that suffered cyber attacks during the period 2004 to 2022. More specifically, statements and questions regarding cyber events are examined to understand the importance of cybersecurity for financial analysts and managers in public channels, such as conference calls. Previous studies have examined firms' 10K disclosure and press releases around cyber incidents (Berkman et al., 2018; Ettredge et al., 2018; Li et al., 2018). Furthermore, we investigate whether financial analysts directly or indirectly inquired top management about cyber breaches in the past years, especially after 2011 when the SEC issued cybersecurity guidance.

Chapter 3 examines how sell-side financial analysts react toward uncertainty or asymmetry as Regulation Fair Disclosure (Reg FD) limits the information exchanged between managers and financial analysts. The analysis relies on a comprehensive dataset from Advisen, a leading data provider for the commercial property and casualty insurance market.[3] Advisen casualty loss data include all the cybersecurity events and class action suits following these events, with the dollar damage estimated at over $1 billion. Advisen gathers its cyber events from different channels, such as public information and certified legal and general news websites. The Advisen database incorporates data obtained from several open-access sources after a thorough review conducted by Advisen insurance experts. The Advisen data collection process necessitates a substantial allocation of labor and does not rely on a single data source that yields insufficient data points.[4] There are also two main components of cyber loss incidents in the Advisen database, including the date of cyber incidents with the estimation of cyber losses such as response cost, reputation loss, and financial damages, as well as the comprehensive details of legal lawsuits related to the cyber incidents.

[3] https://www.advisenltd.com/

[4] https://www.advisenltd.com/data/cyber-loss-data/

Furthermore, Advisen manually codifies and categorizes its casualty loss database accordingly to the severity and types of cyber incidents. [5] The Advisen database is mentioned in an International Monetary Fund (IMF) working paper by Bouveret (2018) as a niche provider of cybersecurity events data besides two other commercial data providers, such as Statistical Analysis System (SAS) and International Business Machines Corporation (IBM).

1.2. Motivation

Empirical evidence shows that cybersecurity events have economic implications for affected firms.[6] In this regard, the Ponemon Institute (IBM Security, 2019) emphasizes that the cost of data breaches primarily arises from implications on a firm's stakeholders (customers, suppliers, employees), negligence in following cybersecurity regulations, and constant change in the security landscape such as the adoption of cloud technology. Besides, the probability of encountering a data breach has also increased over the past few years.[7] According to the same institute, the prominent cause of this upward trend is the adoption of cloud technology in today's digital era. Despite this potential risk, cloud computing technology has become more popular among banks nowadays due to advanced analytics capability and resilience to hacking activities.[8] Hence, the unpredictable impact of cloud technology on banks needs further investigation by analysts to delineate its impact on the probability of breaches, and thus, on bank performance

[5] https://www.advisenltd.com/wp-content/uploads/2016/04/excess-casualty-loss-data-methodology-2016-04-19.pdf

[6] Ponemon's study states that data breach cost increased by more than $370,000 with third-party involvement while rising by $300,000 with the cloud migration.

[7] The percentage change of encountering a data breach increased from 22.6 percent in 2014 to 29.6 percent in 2019 (IBM Security, 2019)

[8] Banking regulators indicate that cloud computing technology has positive impact on the cyber defense due to its resilience to hacking activities and additional features to improve clarity in financial reporting. It is contradictory to the report filed by IBM Security in 2019 because the cloud migration is not easy for banks who are more familiar with legacy banking system (https://www.mckinsey.com/industries/financial-services/our-insights/fast-forward-how-cloud-computing-could-transform-risk-management)

outcomes. While the immediate direct economic consequences of data breaches may not be considered significant, the increasing number of data breaches in recent years has attracted much public attention, including investors and analysts, since it raises uncertainty about the affected firm's prospects.

As financial analysts work to assess firms' prospects, they must estimate and factor in the greater probability of future cybersecurity events, costly legal settlements and ever-tightening regulations. For example, to improve the cybersecurity environment, the SEC proposed amendments to reporting material cybersecurity breaches, which include "periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures."[9] Therefore, cybersecurity incidents present analysts with a significant challenge in assessing a firm's future performance.

1.3. Main findings

The analysis of conference calls in Chapter 2 shows that financial analysts raise additional queries about cyber-related concerns such as digital fraud, cloud technology, or technological investments to encourage top management at Bank of America and Bank of New York Mellon to discuss their cybersecurity risk management and controls. Financial analysts are putting more effort into assessing the cyber safeguard measures at Bank of America and Bank of New York Mellon, most likely due to the JP Morgan Chase cyber occurrences and the reach of New York State law.

[9] https://www.sec.gov/news/press-release/2022-39

Top management and financial analysts paid much attention to cybersecurity disclosures after the SEC issued cybersecurity guidelines in 2011. As credit institutions develop online platforms and cloud technology, financial analysts question the safety of banks' cyber defense mechanisms in conference calls. Since 2014, financial analysts have asked JP Morgan Chase's top management about its mobile platform and bank capital, prompting top management to provide more information about the intended use of capital for cybersecurity investments. The 2017 Equifax data breach prompted analysts to investigate Citigroup's cybersecurity spending approach. Additionally, financial analysts are under public scrutiny to compel Capital One's top management to disclose their cybersecurity risks and controls. Interaction between financial analysts and top managers can help the public gain more insight into banks' cybersecurity management practices.

Chapter 3 examines whether financial analysts benefit from this interaction by incorporating these cybersecurity management practices into their financial valuation model, especially after the occurrence of cyber breaches. More specifically, our study assesses the relationship between cyber incidents and the financial analyst information environment, with uncertainty and information asymmetry as critical dimensions. Financial analysts are more likely to revise their forecasts for banks undergoing cyberattacks than for banks not experiencing cyberattacks. Findings show no significant changes in analyst forecast errors, suggesting that financial analysts do not do a better job after revising their forecasts. However, financial analysts still put significant effort into improving their understanding of the cyber information environment after a cyber crisis, reducing the common uncertainty among their earnings forecasts. However, there are some signs of herding behavior among analysts.

The restricted availability of cyber information in the public domain may pose a difficulty for financial analysts in assessing the extent of cyber breaches, including those resulting in minor damages to financial institutions. Cybersecurity events tend to increase information asymmetry among financial analysts. The lack of clear and consistent cyber management practices during a cyber crisis presents a challenge for financial analysts, thus potentially leading to a greater dispersion in earnings forecasts. Moreover, safeguarding cybersecurity information by management is a common practice to mitigate potential adverse financial consequences, thus further exacerbating information asymmetry.

Finally, reduced information asymmetry mitigates forecasting risks and motivates financial analysts to revise their earnings forecasts. Besides, financial analysts exhibit a tendency not to engage in changing their earnings forecasts in situations where there is a significant information asymmetry.

The specific type of cyber incident also influences analysts' assessment of future bank performance. Measuring the reputation damages associated with confidentiality-related cyber breaches and the minor financial damages resulting from availability-related cyber breaches pose a challenge for financial analysts. As information about banks that have experienced confidentiality breaches is easily accessible in online publications, analysts have reduced information asymmetry. Cyber breaches connected to integrity are uncommon and unpredictable, but cyber breaches related to availability happen regularly. Analysts conclude that the impacts of these two categories of data breaches are difficult to recognize.

1.4. Contribution

The evidence provided in the thesis contributes to the accounting literature and brings insights for managers, investors, and financial analysts. Specifically, chapter 2 contributes to the accounting literature in the following ways. First, the interaction between financial analysts and top management helps us gain insight into the significance of cybersecurity events. Despite disclosure obligations and guidance relating to cybersecurity risks and cyber incidents, the SEC does not set a specific materiality threshold to report security breaches. Financial analysts are more likely to ask direct questions regarding the negative impacts of cyber breaches if they think cyber attacks are important and material. Investors may rely on analysts' expertise to make sense of information such as the number of records exposed, the litigation cost, or cyber loss amounts after security breaches through the earning conference calls to recognize the importance of cyber events. This study examines the potential impact of Reg FD on the cybersecurity market since Reg FD may restrict the flow of information between managers and financial analysts through private meetings. Despite this, direct communications between managers and financial analysts still give financial analysts some advantage over investors in recognizing the important impacts of cyber breaches.

Prior cybersecurity studies focused on the impact of cyberattacks on investors, auditors, top management, and boards of directors. Chapter 2 explores analysts' quarterly interactions with top management (CEO, CFO, and CIO) to exemplify how analysts put pressure on top management to discuss their cybersecurity plans. Therefore, the second contribution of our study is that cyberattacks can signal banks to proactively disclose their cybersecurity procedures within unregulated channels such as earnings announcement conference calls. A prior study by Zafar et *al.* (2012) indicates the positive signals of information security breaches on breached firms compared to non-breached competitors. Thus, our study infers that analysts are concerned about security breaches and raise direct questions related to cyber events within quarterly earnings conference calls. For example, after JP Morgan Chase disclosed its data breach in 2014, analysts have directly inquired about the bank's cybersecurity status, including loss of business income, response costs to cyber attacks, and cybersecurity spending.

Third, prior research finds that investors react negatively to the more explicit textual content of the breach disclosure associated with confidential data leakage (Campbell et *al.*, 2003); however, these reactions may not reflect the true impact of these cybersecurity events. There is barely any evidence to prove that cyberattacks severely influenced Citigroup, Bank of America, and Bank of New York Mellon from 2005 to 2013, according to financial analysts' reactions in earnings conference calls in Chapter 2. While Citigroup suffered several data breaches, the impact of breaches was insignificant compared to security breaches at JP Morgan in 2014. Security breaches at Bank of America and Bank of New York Mellon happened in the early years. However, there were few concerns regarding technological issues back then compared with recent technological trends. Cloud technology, artificial intelligence, or security automation have become more prominent within the banking industry in recent years, especially after 2014. It happened right after one of the biggest JP Morgan cyber incidents.

Chapter 3 contributes to the literature in the following ways. The channel by which the cyber incident affects stock market values is still unclear. By focusing on financial analysts, a key capital market intermediary, this study sheds additional light on information dynamics within the cybersecurity market. In other words, Chapter 3 allows us to understand better how cybersecurity events (including ones without specific breach settlement) impact the economic environment of publicly traded banks, especially concerning the financial analyst that puts some direct pressure on managers by directly asking about the aftereffects of the cybersecurity breaches. Additionally, we examine how sell-side analysts, as sophisticated participants in the capital markets (e.g., Ramnath et *al.*, 2008), incorporate the impact of cybersecurity events after quarterly conference calls into their likelihood of revision in Chapter 3 of this study.

Chapter 3 investigates how sell-side analysts, as sophisticated participants in the capital markets, incorporate the impact of cyber events in their decision-making. Financial analysts must differentiate between informative public disclosure and the noise of boilerplate cybersecurity disclosure, which has no predictive value (Hilary et *al.*, 2016). As financial analysts are the information intermediary, they must play a role in navigating the stock market reaction based on their earnings forecast for the next few quarters.

The prior research on cybersecurity events mostly finds an adverse stock market reaction after security breaches related to privacy, software vulnerability, viruses, and reputation losses (Acquisti et *al.*, 2006; Campbell et *al.*, 2003; Cavusoglu et *al.*, 2004; Hovav et *al.*, 2003; Hovav et *al.*, 2005; Telang et *al.*, 2007; Zafar et *al.*, 2016). Other studies do not find a statistically significant market reaction to data breach incidents related to hacking activities and prior cyber disclosure (Hovav et *al.*, 2004; Hilary et *al.*, 2016). The unpredictable market reaction to cyber incidents shows high market uncertainty among investors. Chapter 3 focuses on the potential sources investors might rely on to make better financing decisions. The impact of adverse cybersecurity events will go beyond the negative market reaction and include reputation losses, loss of business income (loss of customers), and legal settlement of the breach, which might not be predictable and easily discovered publicly. However, analysts' forecasts can reflect the severity of cybersecurity events on firm prospects through the likelihood of revision and analyst forecast properties such as uncertainty and information asymmetry among financial analysts. Finally, Chapter 3 extends prior work on the moderating role of analyst coverage in reducing information asymmetry by examining analyst forecast revision’s likelihood, timeliness, and analyst forecast properties.

2. Interaction between managers and financial analysts after cyber attacks

2.1 The goal of the case study

This case study focuses on U.S. banks as much client-sensitive information links with other industries, such as the retail industry, where clients use their credit cards for regular purchases and the manufacturing industry, where suppliers use credit systems for payments. These U.S. banks are known for their popularity and high reputation across the U.S. and are visible targets for hackers. Furthermore, the banking industry belongs to the financial category, which incurs the second-highest average data breach cost according to the IBM 2022 report.

INSERT FIGURE 1 ABOUT HERE

Although the healthcare industry reports the highest average data breach cost among all industries (an average of $10.10 million per incident in 2022), it is characterized by strict regulations. It is recognized as an important part of the United States' critical infrastructure. Consequently, confidential information in the healthcare sector is often limited and not easily discovered in conference calls compared to the financial sector. Therefore, our study pays more attention to readily available bank conference calls. Based on the Advisen database, 98 credit institutions have experienced more than one cyber event between 2007 and 2022. While the 90th percentile of the number of cyber events for these credit institutions is 88, the 75th and 50th percentile are 17 and 5, respectively. Therefore, we conclude that hackers tend to focus more on the top credit institutions, and our study focuses on these institutions, especially national and state commercial banks, with available online publications. Citigroup experienced 88 cyber events, and the 2011 data breach affected 360,069 customers. For the banks that suffered more than 88 cyber events in the Advisen database, JP Morgan, Bank of America, Ally Financial, Capital One and

Comenity Bank had more than 200 cyber events. Among these banks, we only focus on JP Morgan, Bank of America and Capital One in our case study as data breaches at these three banks affected millions of customers across the U.S. JP Morgan, Bank of America and Capital One had 406, 335 and 256 cyber events, respectively. On the other hand, Ally Financial suffered a data breach in 2022; however, they successfully resolved their legal lawsuit related to this breach with no significant financial damages. Using Google search, we found no publications regarding cyber breaches at Comenity Bank.

According to the Advisen database, Wells Fargo and Discover Financial Services (DFS) had 139 and 177 cyber events, respectively. While the data breach at DFS only affected 500 residents in 2019, the cyber breach at Wells Fargo affected 50,000 customers in 2017.[10] The number of customers affected by the data breach at Citigroup in 2011 is more than five times the number of customers affected by the data breach at Wells Fargo. For the banks that experienced less than 88 and more than 17 cyber events, data breaches at Bank of New York Mellon and Suntrust Banks affected millions of customers. However, we focus on the Bank of New York Mellon as their affected customers are more than 12 times those of Suntrust Banks (12.5 million vs. 1.5 million). As a result, our case study investigates more significant data breaches at Citigroup. Our study focuses on five major U.S. banks: Bank of America, Bank of New York Mellon, Citigroup, Capital One, and JP Morgan Chase.

This case study cross-examines financial analysts' direct and indirect questions regarding cybersecurity matters in earnings conference calls of these financial institutions from 2004 to 2023. By covering an extensive period, this study intends to investigate which type (direct or indirect) of questions financial analysts react to toward substantial cyber breaches. Moreover, we chose the

[10] https://www.idtheftcenter.org/post/wells-fargo-data-breach-not-your-typical-breach

case study research approach to increase the practical relevance of the role of financial analysts in distributing information about cybersecurity events. Earnings conference calls are valuable information since they are conducted four times a year and have no specific regulations other than Reg FD. It prevents banks from selectively disclosing material information to analysts or institutional investors.

We investigate further what kind of questions analysts ask during the conference calls to investigate the intention of those analysts under Reg FD requirements. We categorize direct questions as the analyst's intention to inquire about cybersecurity investments or breaches. Meanwhile, the indirect question is defined as questions regarding other financial issues. Still, it leads managers to disclose their cybersecurity status.

According to the final rule of selective disclosure and insider trading[11] by the SEC, firms must first inform the public via press releases of this private information before interacting with analysts via quarterly earnings conference calls. This case study investigates evidence that financial analysts are aware of cyber attacks and interact more with top management during earnings conference calls.

2.2 Cyber attacks on the rise

With the rising number of cyber breaches, according to IBM's cost of data breach report from 2016 to 2022 (IBM Security, 2022), cyber events in the financial industry have attracted more attention from the public. The industry figures are among the top three regarding average data breach cost. Data breach costs increased significantly in 2021, probably as the Covid-19 pandemic led to an increase in remote work and cyber vulnerabilities of online meetings and work-related

[11] https://www.sec.gov/rules/final/33-7881.htm

tasks. In 2022, the data breach cost did not increase as much as in 2021, as the U.S. government removed the mandatory isolation requirement and encouraged people to blend into the community again. However, digital transformation is much more demanding now as remote work is the new reality for most institutions (IBM Security, 2022).

INSERT FIGURE 2 ABOUT HERE

The average total cost of a data breach increased from $4.24 million to $4.35 million from 2021 to 2022, according to Figure 1. Based on Figure 1, there was a slight decrease in the average cost of a data breach from 2019 to 2020 from $3.92 million to $3.86 million due to the adoption of security automation. This slight decrease indicates that firms, especially financial institutions, have paid more attention to cybersecurity controls. Data breach costs increased gradually from 2017 to 2020 ($3.62 million to $3.86 million).

Discovering cyber attacks is also essential to financial institutions as the average time to identify and contain data breaches for the financial industry is the lowest compared to other sectors, as shown in Figure 2 in 2020. Cyber attacks raise many concerns, especially for credit institutions such as commercial and investment banks with sensitive customer information, motivating them to respond more quickly to protect customer identity.

INSERT FIGURE 3 ABOUT HERE

However, the average time to identify and contain data breaches has increased from 257 days in 2017 to 287 days in 2021, as shown in Figure 3. This trend indicates difficulties in improving the cybersecurity response team.

INSERT FIGURE 4 ABOUT HERE

Cloud migration and third-party involvement increased average data breach costs by $284,292 and $16.9 million, respectively, according to Figure 4. In most cases, the security system complexity is the factor most responsible for the increase in average data breach costs, as shown in Figure 4. Compliance failures and security skills shortages are other factors causing the average data breach cost increase. Based on Figure 4, extensive encryption and employee training reduce average data breach costs by $252,088 and $247,758, respectively. According to the cost of data breach report (IBM, 2022), the positive effect of adopting security automation and zero trust security approach starting from 2021 will help reduce the data breach cost despite the immediate concern of security skills shortage in 2022.

INSERT FIGURE 5 ABOUT HERE

These facts motivate this study. Specifically, this case study examines how financial analysts seek information about the adverse effects of security breaches by interacting with the CEOs of commercial and investment banks and their response cybersecurity teams, including their Chief Information Security Officer (CISO/CSO), Chief Information/Technology Officer (CIO/CTO), and Vice Presidents (VP), during the Q&A (Questions and Answers) section of the conference calls. In other words, this study examines the demand for cyber-related information from financial analysts at five credit institutions, including Bank of America, Bank of New York, Citigroup, JP Morgan, and Capital One. Based on their NAICS codes (522110), all credit institutions are involved in commercial banking. Among these five credit institutions, JP Morgan and Capital One engage in activities other than depository functions, including investment banking and consumer lending, as indicated by their respective NAICS codes (5523150 and 522291). Third-party involvement generates more uncertainties as financial institutions might not have complete control. Globally, credit institutions such as Bank of America, Capital One, Citigroup, and JPMorgan Chase collaborate with numerous technology providers, software companies, and retailers.[12] Thus, they have high risks of cyberattacks; therefore, our case study focuses on these institutions, especially five credit institutions whose reputations are under public scrutiny after cyber breaches.

2.3 Why do credit institutions attract financial analysts' discussion regarding cyberattacks?

According to IBM's cost of data breach report from 2016 to 2022, extensive use of mobile platforms and extensive cloud migration increase the firms' cyber vulnerability. The information regarding employee cloud migration has been discussed several times during conference calls with credit institutions. In the third quarter of 2019, Sanjay Sakhrani from Keefe, Bruyette & Woods, Inc. asked the CEO of Capital One to give an update on the bank's progress of cloud migration in the third quarter of 2019:

"*I know Scott talked about this at a conference, but I just wanted to get your perspective on the cybersecurity incident. I know there's been some questions on the cloud migration as a result of it, and I was just wondering if you could just give us your updated views.*" (Factset Callstreet Capital One, October 2019)

Richard D. Fairbank, the CEO of Capital One, denied the adverse impact of cloud migration on the data breach incident in October 2019:

[12] https://www.partnerbase.com/bank-of-america
https://www.partnerbase.com/citi
https://www.partnerbase.com/capital-one
https://www.partnerbase.com/jp-morgan

"*Sanjay, with respect to the public cloud and the cyber incident, while the event occurred in the cloud, the vulnerability that led to our breach is not specific to the cloud and could have happened in an on-premises data center environment.*" (Factset Callstreet Capital One, October 2019)

Third-party involvement generates more uncertainties as financial institutions might not have complete control. Globally, credit institutions such as Bank of America, Capital One, Citigroup, and JPMorgan Chase collaborate with numerous technology providers, software companies, and retailers.[13] Thus, they have high risks of cyber attacks; therefore, our case study focuses on these institutions, especially five credit institutions whose reputations are under public scrutiny after cyber breaches.

Furthermore, as credit institutions adopt their mobile platform for their customers' daily transactions, data breaches have presented significant problems in figuring out the best cyber solutions for their technological platforms. John C. Gerspach, a CFO of Citigroup, focused on digital and mobile investment in enhancing customer services. John Eamon McDonald from Sanford C. Bernstein & Co. LLC asked him a question in the first quarter of 2018 as follows:

"*And is there also – just one more on this. Do you have some kind of uptake in mobile adoption and maybe planned shrinkage of call centers or data centers related to this that will pick up in later years?* (Factset Callstreet Citigroup, April 2018)

On the other hand, IBM also claimed that the reduction in data breach costs is due to the success of cybersecurity controls, including employee training, extensive use of encryption, and incident response teams (IBM Security, 2022). Based on Figure 4, extensive encryption and

[13] https://www.partnerbase.com/bank-of-america
https://www.partnerbase.com/citi
https://www.partnerbase.com/capital-one
https://www.partnerbase.com/jp-morgan

employee training reduce average data breach costs by $252,088 and $247,758, respectively. According to the cost of data breach report (IBM, 2022), the positive effect of adopting security automation and zero trust security approach starting from 2021 will help reduce the data breach cost despite the immediate concern of security skills shortage in 2022.

The gap between firms that fully deployed security automation and those that did not deploy is very high over the three straight years from 2020 to 2022. Therefore, artificial intelligence or security automation helps the firm improve its active cybersecurity controls instead of relying only on passive preventive measures such as extensive use of encryption. In recent years, many credit institutions have utilized artificial intelligence in their daily operations to enhance customer services. For example, analyst Mike Mayo from Wells Fargo Securities LLC asked a question about technology investment in the second quarter of 2019:

"Can you talk about technology spend and where you are in the process and priorities for the back-office and the front-office…And then, just overall with total tech spend and where you are in terms of spending or reaping the benefits of past spend?" (Factset Callstreet JP Morgan, July 2019)

Jamie Dimon, the CEO of JP Morgan Chase, emphasizes the vital role of artificial intelligence (AI) in reducing fraud costs:

"*Look, it's amazing, our fraud costs with all the things going on in the world today are down because of effectively for the AI and big data and stuff like that.*" (Factset Callstreet JP Morgan, July 2019)

Therefore, the technology investment might have the opposite effect on the probability of cybersecurity breaches. The judgment on the change in the probability of security breaches requires more effort and data collection by financial analysts, especially through the interaction between financial analysts and top management via earning conference calls.

2.4. Financial analysts’ awareness of banks’ information technology investments

During the past decade, as reflected in the content of earnings conference calls, financial analysts have been putting increasing pressure upon management to disclose more about information technology (digital) investments. For instance, in the fourth quarter of 2014, Goldman Sachs & Co.'s financial analyst Ryan M. Nash questioned Capital One's top management regarding their investments in digital platforms:

“Got it. And, Steve, Rich has talked a lot about digitization. Can you size for us how big these costs are and over what timeframe? We've seen a lot of other banks try to self-fund a lot of these investments and to what extent do you think you can self-fund these?” (Factset Callstreet Capital One, October 2014)

The CEO of Capital One responded to this question by emphasizing the important role of digital investment in the upcoming years:

“So it's more and more becoming, over a longer period of time, who we are in terms of how we operate and how we make decisions and how information is used in the company. ... the thing that led me to go out and build Capital One in the first place was looking at how information and technology we're going to transform, starting with the card business and ultimately banking.” (Factset Callstreet Capital One, October 2014)

In the third quarter of 2016, Bank of America's CEO emphasized the importance of cybersecurity in response to a question regarding digital platforms posed by Nancy Avans Bush from NAB Research LLC:

"Cybersecurity, theft of cards from other people and sold on the Internet, all that stuff is important to us. And so we spend, as we said, $0.5 billion a year protecting ourselves" (Factset Callstreet Bank of America, October 2016)

In the fourth quarter of 2017, the CFO and CEO of Bank of New York Mellon received two questions regarding the purpose of their technological investments from financial analysts Mike Mayo from Wells Fargo Securities LLC and Glenn Schorr from Evercore ISI:

"How should we think of the $250 million extra technology investment relative to that $2 billion base, because it might not be apples-to-apples in that comparison?"- Mike Mayo

"Could you talk at a high level of the money that you have earmarked, is it technology and investments for expanding and improving your current mix of businesses?" – Glenn Schorr (Factset Callstreet Bank of America, January 2017)

Responding to these concerns, they elaborated on their plans to enhance digital infrastructure in the coming years. JP Morgan Chase's top management was asked about digital investments in 2018. In the first quarter of 2019, financial analyst Gerard S. Cassidy from RBC Capital Markets LLC posed a question regarding technology issues:

"And then following up on some comments you made at Investor Day and, I believe, touched on today about technology spending. If I recall correctly, next year, technology spending should be self-funding and stabilized at just about where you are today. When you compare it to the past five years, what has changed where the growth trajectory of technology, nominal dollars, has now kind of stabilized versus what it was like again in the past five years?" (Factset Callstreet JP Morgan Chase, April 2019)

Moreover, in the second quarter of 2019, financial analyst Mike Mayo from Wells Fargo Securities LLC asked a specific question regarding short, medium and long-term technological investment plans to the top management of Citigroup:

"*And then, the longer term question is, how much runway do you have left with technology to improve Citigroup's efficiency? Mark, when you mentioned the levers that help meet your targets, the RoTCE target of 12%, you didn't mention technology, yet you mentioned the $300 million spread between the savings from the investments over the new investment levels"* (Factset Callstreet Citigroup, July 2019)

This question prompted the top management at Citigroup to disclose the advantages of investing in digital technologies and their strategies for enhancing technological infrastructure in 2020. Financial analysts have increasingly recognized the growing significance of digital critical infrastructure in the banking industry in recent years.

2.5. Demand for financial analyst intermediary role in investigating the impact of cyber attacks

Managers are motivated to interact with financial analysts due to analysts' strong ties with institutional investors and their extensive channel for distributing business-specific studies (Bradshaw et *al.*, 2017). By investigating the communication between top management and financial analysts, our case study illustrates the importance of the financial analyst intermediary's role in well-functioning capital markets concerning cyber breaches in the banking industry. Cybersecurity hazards have influenced the traditional model of banking procedures in the financial sector over many years, as they might interfere with the banking system and trigger significant direct and indirect financial losses. (Uddin et *al.*, 2020). For example, cybercriminals may hack the banking system by hindering the transfer of capital between banks, stealing sensitive information, and destroying other businesses with integrated banking services (Uddin et *al.*, 2020). As part of their intermediary role in capital markets, we expect financial analysts to analyze the impact of direct and indirect cyber losses in the banking industry.

Based on Figure 5 regarding the direct and indirect costs of cyber breaches by country, direct costs in the U.S. are the second highest compared to other countries, with $88 million. However, the U.S. took the lead in indirect ($154 million) and total ($220 million) cyber breach costs. The magnitude of costs in the U.S. market suggests that financial analysts should focus on indirect costs rather than relying upon direct costs that may be more easily found in company documentation or other public sources of information. Due to the uncertain cyber information environment, it appears that both direct and indirect costs are not disclosed thoroughly within public channels such as 10K or press releases.

INSERT FIGURE 6 ABOUT HERE

Most direct costs from a cyber breach usually take two forms: settlement of legal claims (e.g., class action suits) and regulatory fines and penalties. For example, following a major cyber breach that led to the data loss of about 147 million clients, Equifax Inc. is estimated to have spent more than $650 million (direct cost) for additional security investments and to settle lawsuits and product liability claims. Similarly, a data breach at Target costs the firm $292 million to settle claims and pay damages of $40 million to customers (Zafar et *al.*, 2016). Other major cyber incidents led to significant costs at Yahoo ($117.5 million), Uber ($148 million), and Home Depot ($17.5 million).[14] Illustrating another source of costs, in 2019, Capital One, a large credit card

[14] https://www.reuters.com/article/us-verizon-yahoo-idUSKCN1RL1H1
https://www.reuters.com/article/us-uber-databreach-idUSKCN1M62AJ
https://www.reuters.com/article/us-home-depot-cyber-settlement-idUSKBN2842W5

issuer, was hit with an $80 million fine by the U.S. bank regulator following a personal data breach involving 100 million clients.[15] Since most credit institutions store vast amounts of detailed and sensitive personal information about their clients, a breach's potential impact and costs can be significant for them.

Based on different cost components listed on IBM reports from 2019 to 2022 (IBM Security, 2022), lost business and post-breach costs are related to the indirect cost of data breaches. Both lost business and post-breach costs belong to the financial loss firms suffering from cyber attacks. They are difficult for individual investors to estimate correctly. Cyber breaches also lead to significant indirect costs for affected firms. Such costs arise, among other things, from the unapproved use of customer information, which could result in long-term deterioration of the firm's reputation.

Malicious activities by hackers to exploit client-sensitive information in cases like Equifax, Uber, Yahoo, Target, and Home Depot also have serious economic consequences via long-lasting reputation losses, which translate into a loss of business income or financial damages. According to the Advisen database, financial damage to Uber Technologies Inc. (2015) and Yahoo Inc. (2016) was around $20 million and $50 million, respectively. Home Depot and Target were estimated to suffer financial damage of $27 million and $5 million following data breaches.

Hackers' activities in 2019 increased by more than one-fifth compared to 2014 (IBM Security, 2019). The life cycle of malicious breaches, which spans from the first notice date to the legal settlement date of the breach, is usually more than 10 percent longer than the average data breach life cycle in the breach report by IBM in 2019. Thus, the 2019 cost of data breach report shows difficulties for firms in recovering from these cyber attacks as these cyber breaches take a

[15] https://www.reuters.com/article/us-usa-banks-capital-one-fin-idUSKCN2522DA

long time to settle legal claims. Thus, the post-breach cost usually increases if there are a lot of legal lawsuits to settle.

After security breaches, there are doubts that some managers have incentives to hide negative immaterial cyber information in public to delay adverse market reactions. According to prior studies (Campbell et *al.*, 2014; Filzen, 2015; Filzen et *al.*, 2016; Gordon et *al.*, 2010; Kravet et *al.*, 2013; Li et *al.*, 2018), firms who have experienced security breaches would like to improve their image by releasing more disclosure about the cybersecurity. It is difficult to identify whether managers intentionally conduct this behavior; however, investors might identify the impact of cybersecurity events through analysts' interactions with managers in quarterly earnings conference calls.

Direct costs toward security breaches, such as regulatory fines and financial damages, might be estimated in the press release. However, indirect costs such as response, lost business, and legal expenses are more difficult to measure. By investigating the interaction between managers and financial analysts in earnings conference calls after cyberattacks, this case study examines whether and how financial analysts consider cyberattacks significant by interrogating the managers and whether management discloses cybersecurity information without being prompted directly.

2.6. The challenge and role of voluntary disclosure in investigating the impacts of security breaches

2.6.1. Regulation Fair Disclosure, financial analysts, and cybersecurity puzzle

According to the Regulation Fair Disclosure (Reg FD), material non-public information must be disclosed to investors via public channels. Material non-public information is no longer permitted between managers and financial analysts through private meetings. Due to the absence of discreet ways to interact between managers and analysts, Reg FD increases analysts' dependency on publicly available information when formulating their forecasts (Kross et *al.*, 2012).

This may increase dispersion in analyst earnings forecasts. However, managers still have different ways to give an advantage to financial analysts via conference calls and private meetings after the Reg FD in 2000, which encourages financial analysts to stay on the "good side" of managers (Bradshaw et *al.,* 2017). Our case study investigates cybersecurity information exchanged between financial analysts and managers to understand this interaction after Reg FD from 2004 to 2023.

Our study analyzes direct or indirect pressure by financial analysts to inquire about cybersecurity information, especially during cyber breaches. There are no specific regulatory requirements or thresholds for material cybersecurity disclosures. Therefore, cybersecurity information is often found in 10K reports based on SEC cybersecurity guidelines.

Reg FD may reduce the quantity of information financial analysts provide in the financial market as they limit the source of information from the managers (Kros et *al.*, 2012). Some other studies (Campbell et *al.*, 2021; Koch et *al.*, 2013) indicate the chilling effect within the financial market, where individual investors and financial analysts have an equal opportunity to gather the most efficient information in public channels. However, regulators still allow managers to disclose immaterial private information even though it becomes valuable when combined with financial analysts and investors' proprietary information (Campbell et *al.*, 2021).

The public discussion on security roadmaps might attract more attention from hackers. This expectation may lead to more cautious cyber disclosures by managers. Nevertheless, managers want to disclose material cybersecurity risks and controls through conference calls to reap the benefits of transparent disclosure to investors (Lambert *et al*. 2007). In this scenario, investors indirectly benefit from the pressure of analysts on top management via quarterly earnings conference calls. As financial analysts are privileged to interact with managers via voluntary disclosure such as earnings conference calls or private meetings, they may have some informational benefits over investors. Furthermore, they also pay attention to their performance as compared to their peers in the financial market by revising forecasts based on the quality of information they gather from different sources (Stuerke, 2005); as a result, there is a demand for financial analysts' intermediary role in the financial market in the event of cyberattacks.

2.6.2. Conference calls as a means to improve cybersecurity management practice

The quarterly earnings conference call transcripts show the public interaction between managers and sell-side financial analysts. As a result of Reg FD enforcement, financial analysts must use other sources of information, such as firms' earnings disclosures and quarterly earnings conference calls to update their earnings forecasts (Kross et *al.*, 2012). Therefore, managers often give quarterly earnings conference calls to improve analyst earnings forecast accuracy to cover up for the lack of private information between managers and financial analysts.

Our case study suggests that security breaches trigger financial analysts to ask questions during earnings conference calls. Although it might not be feasible to fully discover how financial analysts and managers react toward security breaches, our case study aims to understand the meaning behind the interaction between financial analysts and top management during earnings conference calls. The higher uncertainty among financial analysts due to the absence of private interaction between managers and financial analysts after Reg FD encourages managers to provide value-relevant information for financial analysts regarding security breaches via conference calls. Managers rely on earnings conference calls to relay messages to financial analysts.

2.7. Case study analysis of five credit institutions

2.7.1. Latest financial analyst concern regarding cyber attacks within Bank of America

In the early stages of cyber incidents for Bank of America, the analysts were not concerned about the negative impacts of these events even though the bank experienced different types of cyber-attacks according to Advisen (Privacy - Unauthorized Contact or Disclosure, Identity - Fraudulent Use/Account Access, Data - Physically Lost or Stolen, Data - Malicious Breach).

However, not all security breaches are disclosed via press releases. For example, only data breaches in Bank of America in 2005, which affected 1.2 million accounts, including Social Security numbers, were revealed in a news release.[16] Furthermore, sell-side financial analysts did not ask specific questions regarding cyberattacks in the quarterly earnings conference calls in 2005. It seems that, despite the enforcement of Reg FD in 2000, Bank of America managers are reluctant to disclose their security breaches in public channels. Financial analysts also did not inquire with top management regarding cybersecurity information in 2012 and 2023, the most recent cyber incident of Bank of America.[17]

Instead, financial analysts chose indirect methods to ask about cyber breach information. For example, in the third quarter of 2016, Nancy Avans Bush from NAB Research LLC indirectly inquired about potential digital frauds:

[16] https://www.cbsnews.com/news/bank-of-america-security-lapse/
[17] https://www.bankinfosecurity.com/bank-america-responds-to-breach-a-4487
https://www.privacyaffairs.com/bank-of-america-database-leaked/

"And I guess my question to you would be as you move more to digital methods of attracting customers and keeping customers, et cetera, I mean is fraud on either side becoming a bigger issue? Or if you could just speak to the whole issue of how you prevent fraud as you become a more electronic bank." (Factset Callstreet Bank of America, October 2016)

Financial analysts from NAB Research LLC were worried about potential frauds in today's digital era when banks adopt more electronic methods to facilitate their daily banking operations with customers. In 2005, bank customers might not have heard of online deposits or transactions. Nowadays, everything can be done quickly with a button online. As a result, digital fraud has become more and more prevalent. Bank of America's Chief Executive Officer (CEO) proactively responded to Nancy Avans by ensuring the safety of the bank's electronic system.

In the third quarter of 2018, the CEO continued to emphasize the bank's ongoing investment in controlling cyber risks to respond to the question by Gerard Cassidy from RBC Capital Markets LLC as follows:

"Can you share with us what risks you're kind of looking out for on the horizon?" (Factset Callstreet Bank of America, October 2014)

The CEO showed a willingness to share more about cybersecurity risks with financial analysts as cyber attacks have attracted much attention from the public. Since analysts have started paying more attention to fraudulent risk management within the digital banking industry, top management is encouraged to relieve pressure by disclosing their ongoing cybersecurity investment to cope with future security breaches. This evidence suggests that indirect questions by analysts regarding fraud may result in more management disclosure of cybersecurity within the earning conference call of the banking industry.

One exceptional case related to cyber attacks happened in 2014 when financial analyst Guy Moskowski from Autonomous Research US LP directly inquired about Bank of America regarding cybersecurity investments. He was interested in their strategy against one of their competitors, JP Morgan Chase, which just suffered cyber attacks in 2014:

"JPMorgan has discussed a $250 million budget for cyber security issues, which is expected to double. Can you give us a sense for what you're spending there and how you would expect it to increase?" (Factset Callstreet Bank of America, October 2014)

Then, Bank of America CEO Brian T. Moynihan responded to this question by pointing out the cybersecurity talents within the board and technology team and their active cooperation with government agencies to fulfill cybersecurity guidelines set by the SEC. Because banks were susceptible to high cyber risks due to their continuous digital transformation and software upgradation, sell-side financial analysts paid more attention to how banks manage their cybersecurity risks and controls. This change was possible due to the update in the SEC cybersecurity guidance in 2011 or the significant rise in cyber attacks after 2011. However, the study cannot confirm that financial analysts' changes in behavior are due to changes in guidance or information security environment. Our study concludes that financial analysts have paid more attention to the impact of more significant cyber breaches related to JP Morgan Chase than minor cyber breaches related to Bank of America that happened at least once a year.

2.7.2. The impact of regulation on financial analysts regarding cyber attacks within Bank of New York Mellon

Advisen indicates that Bank of New York Mellon has suffered cyber attacks from 2008 to 2017 with different cyber attack types such as Data - Physically Lost or Stolen; Privacy -

Unauthorized Contact or Disclosure; Data - Unintentional Disclosure; Data - Malicious Breach. However, press releases issued by the bank only indicate that the personal information of 4.5 million customers was compromised in the Bank of New York Mellon data breach in 2008.[18]

Although the SEC issued cybersecurity guidance in 2011, financial analysts did not ask any specific questions regarding cybersecurity controls until 2017, when New York State adopted cybersecurity regulations to protect financial institutions from malicious activities by hackers. After the SEC proposed new cybersecurity guidance in 2018, financial analysts indirectly asked top management about cybersecurity spending and capabilities. Financial analysts take the more passive approach because top management proactively share cybersecurity information in the management presentation section of quarterly earnings conference calls. In the third quarter of 2016, the CEO of Bank of New York Mellon opened up about their cybersecurity investments:

"Our third priority centers on being a strong, safe, trusted counterparty. During 2016, we invested in and focused on compliance, risk management, and control functions, made significant investments in our resolution and recovery plan, which included submitting an updated resolution plan that adequately addressed the deficiencies that the Federal Reserve and FDIC had previously identified in our 2015 submission. We further rationalized our credit exposure to certain financial institutions and sovereigns, strengthened our risk identification and operational risk control processes, delivered key new capabilities in cybersecurity, and enhanced our capital adequacy process." (Factset Callstreet Bank of New York Mellon, October 2016)

Before 2017, there was barely any discussion between managers and financial analysts regarding network security or information technology security in the bank's earnings conference calls. In the fourth quarter of 2017, Glenn Schorr from Evercore ISI, Mike Mayo from Wells Fargo

[18] https://www.bankinfosecurity.com/bank-ny-mellon-breach-much-bigger-than-first-announced-a-952

Securities LLC, and Geoffrey Elliott from Autonomous Research LLP indirectly inquired top management of Bank of New York Mellon about the investment in technology to cope with future security breaches as following:

"Could you talk at a high level of the money that you have earmarked, is it technology and investments for expanding and improving your current mix of businesses?" – Glenn Schorr- (Factset Callstreet Bank of New York Mellon, January 2018)

"How should we think of the $250 million extra technology investment relative to that $2 billion base, because it might not be apples-to-apples in that comparison?" – Mike Mayo- (Factset Callstreet Bank of New York Mellon, January 2018)

"*You make an investment up front and then it generates revenues in future years. I'm just trying to understand. Do you expect to get a positive earn-back over a certain number of years on these?" - Geoffrey Elliott-* (Factset Callstreet Bank of New York Mellon, January 2018)

After receiving questions regarding technological investment, the Chief Financial Officer (CFO) and the CEO answer the questions above by emphasizing that the banks have spent most of their money maintaining high-quality cybersecurity infrastructure to cope with potential digital frauds and gain customer confidence. Our study concludes that financial analysts pay more attention to the Bank of New York Mellon's preventive measures to deal with potential cyberattacks rather than directly assessing the quality of their cybersecurity defense system. Financial analysts encourage top management to share their cybersecurity investments more willingly by indirectly inquiring about the cybersecurity risk management framework.

2.7.3. Mixed reaction from financial analysts toward the cyber attacks within JP Morgan Chase

Based on the Advisen cybersecurity database, JP Morgan Chase has suffered cyberattacks from 2005 to 2021, with several cyber incidents per year (Privacy - Unauthorized Contact or Disclosure; Data - Physically Lost or Stolen; Data - Malicious Breach; Phishing, Spoofing, Social Engineering; Skimming, Physical Tampering, IT - Processing Errors). Sell-side financial analysts have not interrogated the top management for data breaches from 2005 to 2010.

News agency Reuters only published some news about JP Morgan Chase data breaches in the online platform alongside Kroger in 2010, when customer names and email addresses were claimed to be leaked.[19] However, an event in 2014 has attracted much attention from analysts. The 2014 JP Morgan cyberattack affected 83 million accounts across the U.S.[20] Since then, financial analysts have worried more about the bank's cybersecurity status.

Since the end of 2013, several analysts have asked more cybersecurity questions than the previous year. However, sometimes financial analysts indirectly ask for cyber risks or controls that the bank implemented. Top management, such as the CEO or CFO, is more willing to openly discuss their cyber risk management controls. For example, Erika P. Najarian from Bank of America Merrill Lynch poses a question regarding bank capital buffering in the fourth quarter of 2013:

"Could you remind us of how you're thinking about the benefits of keeping the franchise consolidated for the shareholders versus some of the conversation that investors are having today about breaking up or shrinking the bank in order to step down on your capital buffers?" (Factset Callstreet JP Morgan Chase, January 2014)

[19] https://www.reuters.com/article/us-epsilon-idUSTRE73103G20110402
[20] https://www.reuters.com/article/us-jpmorgan-cybersecurity-idUSKBN0K105R20141223

To respond to this question, James Dimon (Chief Executive Officer) at JP Morgan Chase proactively indicates the vital role of cyber defense mechanisms for the safety of data centers. It might seem irrelevant to mention cybersecurity in the topics of bank capital buffering. However, it is still meaningful for top management to ensure the safety of their digital banking structure, as cybersecurity has an essential impact on the digital transformation process within the banking system.

Meanwhile, in the second quarter of 2016, Marianne Lake (CFO) at JP Morgan Chase actively ensured the high-quality cyber control of the online payment system along with bank cybersecurity investments to maintain this high quality to respond to questions by financial analyst Gerard Cassidy from RBC Capital Markets LLC. In 2016, Gerard Cassidy was concerned about the development of JP Morgan's mobile platform:

"Can you share with us, the update on clear exchange? It's expected to be rolled out later this year, and what that might do to even grow the mobile business even more than it's growing now?" (Factset Callstreet JP Morgan Chase, July 2016)

The mobile infrastructure required investments in cybersecurity; therefore, the question about mobile businesses triggered top management to share more about their cybersecurity investments. During the conference calls, financial analysts unintentionally encouraged JP Morgan Chase's top management to pay more attention to their cybersecurity disclosures. In the fourth quarter of 2016, there was a similar situation regarding the investments in cyber "infrastructure." Erika P. Najarian from Bank of America Merrill Lynch once again asked top management regarding capital budgeting in the fourth quarter of 2016:

I know that you've said previously that regulatory reform or regulatory relief will unlikely have any fundamental change in terms of how you're thinking about budgeting, but I'm wondering *if you could help us understand over the past few years, how much have regulatory costs grown?* (Factset Callstreet JP Morgan Chase, January 2017)

To respond to this question, Marianne Lake (CFO) at JP Morgan Chase provided more details of JP Morgan's plan to strengthen digital infrastructure. At the end of the year 2020, Glenn Schorr from Evercore ISI asked top management about the benefits of data analytics using machine learning and artificial intelligence in today's digital era:

"I'm just curious, we haven't heard that much lately about what you're collecting, how you can use it, how you can use it to enhance the customer experience, accelerate growth. You have all this at your fingertips and people talk about data as being the new gold." (Factset Callstreet JP Morgan Chase, January 2021)

Jamie Dimon reassured investors about the bank's proactive cyber risk management through information technology talents and data analytics using artificial intelligence. Recognizing the importance of human factors in reducing the negative impacts of cyber attacks, top management at JP Morgan Chase switched their focus to hiring employees specializing in cybersecurity rather than only focusing on improving digital infrastructure. Financial analysts successfully obtained more information regarding JP Morgan Chase's plans to improve its cyber defense mechanism.

In the first quarter of 2022, Betsy L. Graseck from Morgan Stanley & Co. LLC asked about the bank's achievement in the payment category, while Mike Mayo from Wells Fargo Securities LLC was more interested in a risk management system during the economic recession:

"So could you give us a sense as to where you think you are in this total payments category you're talking about, what you're expecting in terms of drivers to get to double-digit and what

kind of timeframe you're thinking about there?" - Betsy L. Graseck- (Factset Callstreet JP Morgan Chase, April 2022)

"Do you think the US is going to have a recession this year based on everything you know?" - Mike Mayo- (Factset Callstreet JP Morgan Chase, April 2022)

Jamie Dimon (CEO) explained the bank's efforts to cope with the continuously changing economic landscape, such as spurring real-time payments or the Ukrainian war. Indirect behaviors by financial analysts could often act as an unintentional action to encourage more cybersecurity disclosures within earnings conference calls.

Among depository and non-depository institutions that have experienced cyberattacks from 2004 to 2020, JP Morgan has received the most questions from analysts about cybersecurity. JP Morgan Chase experienced cyberattacks in 2010 and 2014. The impact of breaches in 2013 was much more significant than in 2010, leading to more interaction between analysts and JP Morgan's managers from 2014 to 2020. Financial analysts are concerned that cybersecurity incidents could negatively influence the banks' business operations. During the third quarter of 2013, both Matt H. Burnell from Wells Fargo Securities and Besty L. Graseck from Morgan Stanley & Co. LLC asked specific cyber-related questions regarding the future forecast of potential card fraud behaviors:

"And then separate topic just on the security breach that you discussed and you indicated that the card replacements that you've done so far has been de minimis in terms of expense. But could you just speak a little bit bigger picture to how you're thinking about fraud in the card space as well as in the debit space?" - Besty L. Graseck- (Factset Callstreet JP Morgan Chase, October 2013)

"And then just finally for me, are you seeing given some of the security breaches not only in your cards but across a couple of other issuers, have you seen any reduction in consumer spending potentially related to that via cards moving to other forms of purchases or is that?" - Matt H. Burnell (Factset Callstreet JP Morgan Chase, October 2013)

The card business was vulnerable to cyber attacks from online criminals, encouraging analysts to discuss this matter more thoroughly when interacting with Jamie Dimon (Chief Executive Officer) at JP Morgan Chase. The theft of confidential data such as the PIN of credit or debit cards and personal information can cause bank clients to lose money on their cards due to fraudulent transactions made by cyber criminals (Uddin et *al.*, 2020). Due to the adoption of online banking platforms, the bank's card business has been highly exposed to cyber risks since 2014. Consequently, financial analysts required more nonfinancial information regarding card business risk management when evaluating the cybersecurity status of JP Morgan Chase. Besides, Ms. Graseck asked top management of JP Morgan Chase further questions on the cybersecurity spending in 2014, which proves that some analysts worried about the impact and preventive cyber measures to avoid future breaches:

"And I think is it accurate, Jamie, that you mentioned at a recent conference that you were looking to double the spend in cyber security. Is that right?" (Factset Callstreet, October 2014)

In the third quarter of 2017, due to the heavy influence of another significant Equifax data breach, Betty Graseck from Morgan Stanley & Co. LLC was concerned about how JP Morgan Chase would respond accordingly to prevent future fraud activities:

"And then the second question is just how you're dealing with the Equifax fallout. The question here is, does the breach that occurred drive any changes to how you are assessing credit requests that come in?" (Factset Callstreet JP Morgan Chase, October 2017)

Marianne Lake (CFO) indicated that banks adopt a constantly upgraded cybersecurity system to alleviate the contagion impact of the Equifax data breach. The Equifax data breach affected millions of customers. It might change the way financial analysts access the cyber risk management at JP Morgan. This cyber breach affected other financial institutions, especially credit institutions with considerable client personal information data. Like other credit institutions such as Bank of America and Capital One, JP Morgan's top management received many questions regarding bank investment in cybersecurity, which the Basel committee demands to cope with the rise of cyber attacks (BIS, 2016). The Basel Committee on Banking Supervision serves as the principal international organization for developing standards related to the prudent oversight of banks, such as Tier 1 and 2 capital requirements (Basel II and III). Additionally, it gives a platform for continuous communication on matters about the regulation of banks.[21]

From 2017 to 2020, there was barely any discussion regarding cyber but rather more discussion regarding technological advances and digital transformation. However, since 2020, financial analysts have been more interested in cyber risk management and controls due to the adoption of digital transformation and artificial intelligence software. At the end of 2019, Glenn Schorr from Evercore ISI asked top management of JP Morgan Chase regarding the data providers and artificial intelligence:

"Quick question on open APIs and what the big picture is here and how it impacts you and the rest of the banking industry, meaning there are concerns over data security and things like that, but JPMorgan has plenty of agreements with some of the bigger providers" (Factset Callstreet JP Morgan Chase, January 2020)

[21] https://www.bis.org/bcbs/

Cyber vulnerability also has been very high nowadays due to the technological advancements in banking, encouraging financial analysts to ask more questions regarding data providers to access the cybersecurity of JP Morgan's daily banking operations. Additionally, most of the data nowadays are imported into the cloud database and analyzed using machine learning and artificial intelligence to develop various solutions for daily banking operations. While cloud databases were vulnerable to cyber breaches, firms used artificial intelligence to cope with cyber attacks (IBM Security, 2022).

In the fourth quarter of 2020, Betsy L. Graseck from Morgan Stanley & Co. LLC also had similar worries about data analytics and cybersecurity:

*"And then the follow-up question just on the technology budget increasing. I mean, I know this comes after a year of being somewhat stable year-on-year. And just wanted to dig into the comment that you made on the page around data analytics, cybersecurity, and artificial intelligence capabilities." (*Factset Callstreet JP Morgan Chase, January 2021)

Then, JP Morgan Chase's CEO gave more comprehensive plans to strengthen the bank's cybersecurity controls over data centers and cloud-based technology to relieve those concerns. Financial analysts put some pressure on the top management of JP Morgan Chase to provide more cyber information to the public. A similar situation happened in the fourth quarter of 2021 when Mike Mayo inquired about JP Morgan Chase's investment in cyber risk management in developing digital environment:

"*Again, just looking for some more specifics at least on digital banking and other tech areas where you expect a revenue pickup, not just – I mean, you mentioned fraud and AML and ransomware and cyber, and that's table stakes as you would say. But as far as actually getting* *revenue growth from your tech investments and starting off with digital banking, which new markets are you entering?"* (Factset Callstreet JP Morgan Chase, January 2022)

Mike Mayo expressed significant concerns regarding fraudulent transactions in digital banking, citing the potential threat of ransomware that could potentially disrupt the banking system. This could result in bank managers needing to pay much money to unlock the virus-infected file. Many businesses impacted by ransomware never expect to receive the decryption key in exchange (Uddin et *al.*, 2020). This potentially significant negative impact on banks' financial performance encouraged financial analysts to pressure bank managers to invest more in cybersecurity. Overall, financial analysts had mixed approaches to gathering cyber information from the top management of JP Morgan Chase. While financial analysts posed indirect questions regarding the bank capital budgeting and digital platform, they expressed more direct concerns regarding the data centers and cybersecurity investments.

2.7.4. Favourable indirect financial analyst approach toward cyber attacks within Citigroup

According to Advisen, Citigroup has experienced cyber breaches from 2005 to 2022 with different types of cyber events such as Privacy - Unauthorized Contact or Disclosure; Identity - Fraudulent Use/Account Access; Data - Malicious Breach; Skimming, Physical Tampering; Phishing, Spoofing, Social Engineering, and Network/Website Disruption. Like JP Morgan, Citigroup has attracted more interest from sell-side financial analysts regarding cyberattacks only since 2013, even though it experienced security breaches in 2011 when its credit card customers' personal information was publicly leaked.[22]

[22] https://www.bankinfosecurity.com/citi-breach-360k-card-accounts-affected-a-3760

Analysts did not ask Citigroup's top management questions regarding cyber breaches during the earnings conference call in 2005 and 2011. Sell-side financial analysts indirectly inquired managers regarding fraud and breach cases one year after their breaches in 2013. Since managers are willing to share more information regarding cyber breaches, the analysts might not need to ask further direct questions. For example, in the third quarter of 2014 and the first quarter of 2022, CEOs of Citigroup disclosed cyber-related issues in their management presentation section of quarterly earnings conference calls:

"*While our expense reduction efforts have been productive, we continue to face pressure related to legal costs and the need to invest in regulatory and compliance as well as the critical need to protect our network from cyber crime*." – Michael L. Corbat (Factset Callstreet Citigroup, October 2014).

"The Russian invasion of Ukraine and the sanctions it triggered unleashed an enormous supply shock on the world, further fueling inflation and placing global growth under considerable pressure. Back recently from seeing clients in Europe and the Middle East, it is security, yet energy, food, defense, cyber or operational resilience that has risen to the top of their strategic dialog." – Jane Nind Fraser (Factset Callstreet Citigroup, January 2022).

Citigroup suffered cyberattacks from the Russian gang due to virus-based attacks in 2009. However, interestingly, financial analysts questioned management on these cybersecurity issues two and four years later.

Citigroup suffered many cyber incidents before 2014, but top management barely discussed this issue in the previous earnings conference calls. In the third quarter of 2019, Brian Kleinhanzl from Keefe, Bruyette & Woods Inc. was concerned about risk management:

"And then just a separate one on – you mentioned that there's a continuing investment in controls and risk in Corporate/Other. Are you close to a point where you've reached a peak on that, and we should expect that to trend down over time? Or is it still something that's increasing?" (Factset Callstreet Citigroup, October 2019)

Mark A. L. Mason (CFO) at Citigroup was willing to share more about the bank's investment in cybersecurity to improve the bank's risk management structure. Cybersecurity was previously discussed, along with the investment in technology. However, Citigroup's risk management framework further investigated cyber risk and controls, especially after the 2017 Equifax data breach. Financial analysts indirectly asked more questions about the risk management framework to extract more cybersecurity information to assess the severity of cyber risks within the Citigroup banking system.

Additionally, there were several discussions about the investment in technology and data quality in the years before 2019. However, the managers and financial analysts have not thoroughly discussed this topic, especially cyber systems. However, since 2020, investment in public cloud technology has posed significant cyber risks to banks. Hence, a Wells Fargo Securities LLC financial analyst, Mike Mayo, inquired about this matter in the fourth quarter of 2019:

"Hi. Can you talk about technology spend and where you are in the process and priorities for the back-office and the front-office? I know it's a broad question. But maybe, for the back-office, like, the number of data centers you have or the percent of workload you intend to move to the public cloud. Or for the front-office, a little bit more color on the relationship with Google and where you expect that to go. And then, just overall with total tech spend and where you are in

terms of spending or reaping the benefits of past spend." (Factset Callstreet Citigroup, January 2020)

Financial analysts indirectly facilitated cybersecurity information exchange between the top management and investors regarding cybersecurity investments. Due to technological advances and digital transformation, online databases have become critical for every financial institution to generate better performance based on previous financial outcomes. For banks or credit institutions with large amounts of personal data, top management allocated their accounting budget to improve the critical cybersecurity infrastructure to prevent future cyber attacks. Mark A. L. Mason (Chief Financial Officer) at Citigroup emphasized the importance of cybersecurity expenses in today's digital era, in the long run, to respond to another question by Mike Mayo in the first quarter of 2022:

"I get it, you have the reg order, you have the transformation, you have business sales You've said you underinvested in the past and everything else. But, I mean, you have 1,200 basis points between your expense and revenue growth. And it just seems so high. But you're also guiding for what I think is, like, 300 basis points of that spread for the full year. So does that mean this is as bad as it gets and that spread should be narrowed?"- Mike Mayo (Factset Callstreet Citigroup, April 2022)

Financial analysts paid attention to the benefits of technology investments. They indirectly pressured top management to provide more details of the credit institutions' expenses. Operation expenses were closely related to cybersecurity investments, so financial analysts extracted more cybersecurity information by questioning the details of Citigroup's expenses rather than directly asking about Citigroup's cyber risk management framework.

Financial analysts were only confronted with the top management of Citigroup directly in 2017 as they were afraid of the contagion effect of the Equifax data breach on the bank's cybersecurity risk management. In the third quarter of 2017, Elizabeth Lynn Graseck from Morgan Stanley & Co. LLCC asked top management of Citigroup about the bank's relationship with Equifax:

"A quick question on Equifax. I believe you're one of the users of Equifax and that you partner with them maybe a little bit more than some of the other credit bureaus. I just wanted to get a sense from you as to any changes that you're making with regard to that relationship post-breach, and then also understand if there's anything different that you do on the retail partner card side given that point-of-sale is one of the ways you acquire customers." (Factset Callstreet Citigroup, October 2017)

The CEO of Citigroup responded passively to the questions by financial analysts and attempted to diminish the potential influence that Equifax has on Citigroup's cyber breach management. However, he did not offer any information about improvements to the cyber defense system that Citigroup will implement in the future. In this case, cyber breaches at the business partner of Citigroup have financial analysts worried that since personal information might be linked between Citigroup and Equifax, confidential data leakage at Equifax might negatively affect Citigroup's cybersecurity system.

Cyber breaches may trigger a domino effect for financial institutions with close connections in customer databases. Financial analysts thus pressure top management to share more about their cybersecurity investments. However, financial analysts did not successfully gather more cyber information from the top management of Citigroup, indicating that direct questions might cause the top management to reluctantly disclose more cyber information to the public.

Overall, indirect questions by financial analysts often resulted in more disclosure of cyber risks and controls by managers. As a result, financial analysts tend to adopt more indirect approaches to gather more information regarding the cybersecurity risk management of the banks.

2.7.5. Significant change in financial analyst approach toward cyber attacks at Capital One

Before the cyber incident in 2019, Capital One had been experiencing security breaches since 2005. However, cybersecurity breaches are not disclosed thoroughly in press releases and earnings disclosures. Financial analysts have enquired about cybersecurity information since 2014. Since the earnings conference calls, cybersecurity risk and controls have attracted more interest from sell-side financial analysts.

In 2019, Capital One experienced one of the most significant U.S. data breaches, which affected 100 million customers' accounts.[23] In 2022, the settlement of legal lawsuits toward this cybersecurity incident was decided, with the cost of $190 million demanded.[24] There is a time gap of three years between the time of cyber events and legal settlement, so it is a lengthy process for individual investors and financial analysts to estimate the indirect cost of cyber breaches.

This cyber incident in 2019 encouraged analysts to proactively ask questions regarding cyber breaches during the third-quarter earnings conference call in 2019. Financial analyst Sanjay Sakhrani from Keefe, Bruyette & Woods, Inc. pressured bank managers to investigate their cybersecurity status after top management disclosed their cybersecurity incident in the previous management discussion section. He posed a question regarding the cloud technology during the

[23] https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
[24] https://www.capitalonesettlement.com/en

earnings conference calls when the public information of the Capital One cyber incident was released:

"I know Scott talked about this at a conference, but I just wanted to get your perspective on the cybersecurity incident. I know there's been some questions on the cloud migration as a result of it, and I was just wondering if you could just give us your updated views" (Factset Callstreet Capital One, October 2019)

After being pressured by Sanjay Sakhrani, Richard D. Fairbank (CEO) shared his opinions further on the relationship between cloud and cybersecurity. The CEO once again emphasized the significance of cloud technology in improving Capital One's cyber management. Because software upgrades related to cloud technology can leave some loopholes in information security systems, analysts are interested in knowing more about the bank's actions and safeguards. This finding is consistent with prior research (Uddin et *al.*, 2020), which suggests that inadequate ethical standards among technical staff can heighten the risk of cyber vulnerabilities.

Financial analyst Sanjay Sakhrani was worried about the cybersecurity capabilities of the Capital One technology team to cope with cyber criminals after Capital One experienced huge cybersecurity breaches in 2019. Capital One was currently using online cloud storage to store client personal information, so he changed their approach to be more direct toward disclosing cyber information during conference calls. He became more direct and focused on a specific segment, such as cloud technology, instead of general information, such as digital investments, as discussed in 2015.

Before this cyber incident happened, Capital One had been experiencing security breaches since 2005. However, press releases and earnings disclosures did not thoroughly investigate cybersecurity breaches until 2019. Financial analysts adopted the indirect approach to enquiring about cybersecurity information in 2014. In the earnings conference calls, cybersecurity risk and controls have attracted more interest from financial analysts due to digital transformation.

In the second quarter of 2015, financial analyst Sameer S. Gokhale from Janney Montgomery Scott LLC indirectly asked about digital investment as he is concerned about the digital risks:

"Thank you for taking my questions. Rich, you talked about your incremental investments in digital and as I look at the banks and you guys, it seems like digital is clearly the Wild West to a certain extent. So when you think about digital investments, how do you think about sizing how much of a budget you want to allocate to those investments?" (Factset Callstreet Capital One, July 2015)

Richard D. Fairbank (Chief Executive Officer) stated that Capital One maintained high-quality digital infrastructure, with ongoing investment in cybersecurity talents and protection. Rather than asking directly about cybersecurity, financial analysts concentrate more on digital investment. It might be early to conclude that financial analysts pay attention to data security via digital investment.

Financial analyst Sanjay Sakhrani from Keefe, Bruyette & Woods, Inc. once again brought up this matter along with cloud technology, an essential component of digital transformation, just right before the Capital One cyber breach at the end of 2018:

"I appreciate the color on the cloud migration and the cost reduction from closing the data centers. I guess two questions on that. One, Rich, can you just talk about what competitive advantage it gives you from moving to the cloud and sort of the functionality there?" (Factset Callstreet Capital One, January 2019)

Recognizing the increase in the probability of cyber breaches at Capital One, Sanjay Sakhrani worried about whether the benefits outweigh the cost of adopting cloud technology, including the increase in cybersecurity risks right before the cyber incident. Online data centers were at risk of cyber attacks. They required top management to strengthen the security and reliability of cloud databases.

Financial analysts' questions regarding digital investments or cloud management appear to encourage top management to share more about their cybersecurity information before the 2019 incident. However, they use a more direct approach when recognizing the high probability of cybersecurity breaches from adopting cloud technology before and after the 2019 incident. This change in approach indicates that financial analysts have become more concerned about the negative impacts of cybersecurity breaches as the risk of cyber attacks has increased tremendously in recent years.

2.8. Summary and Discussion

There were barely any discussions about cybersecurity matters before 2014 for the five banks we considered in this case study, especially for Bank of America and Bank of New York Mellon. Since then, financial analysts have initiated indirect questions regarding cyber-related issues such as digital frauds or technological investments to encourage top management at Bank of America and Bank of New York Mellon to share more about their cybersecurity risk management and controls except when the JP Morgan data breach happened in 2014. This data breach encouraged financial analysts to pressure the top management of Bank of America by asking how they expect to make cybersecurity investments. Rather than explicitly analyzing the quality of the bank's cyber defense system as in the cases of JP Morgan Chase and Capital One, financial analysts were more concerned with the bank's measures to guard against potential cyber attacks for Bank of America and Bank of New York Mellons.

Like Bank of America and Bank of New York Mellon, Citigroup received many indirect concerns from financial analysts regarding cyber-related issues. While Bank of New York Mellon and Citigroup's top management proactively share cybersecurity information in the management presentation of earnings conference calls, Bank of America's top management take a more passive approach. Financial analysts only ask Citigroup's top management directly regarding cyber breaches when there is a potential domino effect for financial institutions that have a partnership with Equifax. This credit reporting agency suffered a huge data breach in 2017.

Among all the five credit institutions in our study, JP Morgan's top management received the greatest number of indirect questions from financial analysts regarding bank capital, mobile platforms, and capital budgeting from 2014 to 2022. Top management at JP Morgan proactively disclosed their cyber preventive measure via artificial intelligence and cybersecurity investments. Furthermore, a cybersecurity incident at JP Morgan Chase disclosed in 2014 motivated financial analysts to ask many direct questions regarding whether top management has good preparation against potential cyber attacks. In other words, JP Morgan received the greatest number of direct questions from financial analysts among all five banks in our case study.

Since 2014, JP Morgan's card business has faced significant exposure to cyber risks due to the widespread adoption of online banking platforms. Financial analysts exhibited a significant interest in nonfinancial data of card business risk management while assessing the cybersecurity of JP Morgan Chase credit institutions. Most data were transferred into cloud databases and processed using machine learning and artificial intelligence to build numerous solutions for daily banking operations. Cyber susceptibility is relatively high nowadays, prompting financial analysts to ask additional questions about data providers and cybersecurity.

Bank of America's cyber-related issues attracted more interest from financial analysts in 2014, especially when JP Morgan Chase suffered massive data breaches affecting the overall banking industry. Additionally, there was an early sign of financial analysts' involvement in gathering cybersecurity information for the Bank of New York Mellon in 2017, immediately after New York State implemented cybersecurity laws to safeguard financial institutions from dangerous hacking operations. JP Morgan Chase cyber events and New York State regulation caused financial analysts to put more effort into analyzing the cyber safeguard measures at Bank of America and Bank of New York Mellon by asking top management more direct questions regarding their cybersecurity risk management.

Furthermore, due to the SEC guidelines proposed in 2014, financial analysts have paid more attention to cyber discussions in earnings conference calls. In 2017, Citigroup was under public scrutiny when involved with Equifax data breaches, suggesting more direct pressure from financial analysts on top management regarding cybersecurity matters. Due to the constantly changing technology landscape, including cloud technology and digital transformation, financial analysts asked top management more questions about the cybersecurity investments, risks, and controls at Citigroup and Capital One. With their expertise, financial analysts effortlessly bridged the gap between top management and investors by pressuring top management to disclose cybersecurity information.

After the cyber incident, financial analysts adopted a more proactive stance than they did prior to the incident. Before 2019, the top management of Capital One received indirect questions from financial analysts regarding cybersecurity similar to the ones received by the top management of Bank of America, Bank of America Mellon, and Citigroup. However, like JP Morgan Chase's top management, Capital One's top management faced direct pressure from financial analysts after 2019. The direct conversation between Capital One top management and financial analyst Sanjay Sakhrani in the third quarter of 2019 led to more cybersecurity and cloud technology disclosure by top management. In 2019, the CEO and CFO of Capital One disclosed more cyber information to ensure resilience to cope with potential security breaches in order to respond to cybersecurity incidents. Financial analyst Sanjay Sakhrani and CEOs recognized that upgrading software to cloud technology could create vulnerabilities in information security systems.

Cyberattacks prompted analysts to ask more questions about cybersecurity-related information. The change in New York State regulations and the SEC's cybersecurity guidelines also raised financial analysts' interest. The increasing reliance on cloud-based databases, machine learning, and artificial intelligence also affects cyber vulnerability, leading financial analysts to learn more about data providers and cybersecurity. The next study will show that financial analysts are more likely to incorporate the information from conference calls and decide the likelihood of their earnings forecast revision after security breaches.

3. Cybersecurity events generate uncertainty for financial analysts

3.1. Literature Review

3.1.1. The impact of cybersecurity risk disclosure on financial analysts and investors

Prior research on cybersecurity risk disclosure tends to focus on investors and stock market reactions, neglecting implications for other stakeholders. Evidence from prior research is far from consistent. According to Kravet and Muslu (2013), more risk-related sentences in voluntary disclosure of cyber risks tend to increase stock volatility and trading volume. Their findings imply that increased disclosures falsely enhance investors' risk assessments of cybersecurity defense despite its quality and that risk disclosure at a firm level tends to be boilerplate, casting some doubt on the benefits of greater transparency.

By contrast, Li et *al.* (2018) mention that managers are more likely to increase their firm's cyber risk disclosures or respond to SEC comment letters to catch up with their peers' risk management strategy and relieve some of their financial constraints when borrowing. Moreover, a prior study shows the usefulness of additional voluntary information to the perception of cybersecurity risks. Gordon et *al.* (2010) mention that firms that provide voluntary disclosure (e.g., nonfinancial) in 10K reports regarding information security are also more likely to have a positive stock market reaction. In other words, investors consider this valuable voluntary disclosure for their investment decision-making. Berkman et *al.* (2018) suggest that the stock market reacts positively to the improvement of cybersecurity awareness and to the increase in the number of cybersecurity disclosures. Hence, investors value the quality of the additional cybersecurity disclosure by firms.

Further research sheds light on mapping cybersecurity risk disclosure and stock market reactions. For example, Kravet et *al.* (2013) observe that analysts have different opinions about the increase in risk-related sentences, resulting in dispersed analyst forecast revisions. More specific risk factor disclosures give analysts more information to evaluate the firms' cybersecurity. However, analysts are also aware of the possible manipulation of these disclosures to exaggerate a firm's efforts to improve cyber defense and give a false positive market reaction. Li et *al.* (2018) conclude that the SEC 2011 cybersecurity disclosure guidelines weaken the beneficial link between the existence and duration of cybersecurity risk disclosures and later reported cybersecurity events. This is because firms have no specific materiality threshold or disclosure requirements to evaluate their cybersecurity controls. Therefore, it is even more challenging to quantify the impact of security breaches on investors and analysts. Finally, Lawrence et *al.* (2018) find that risk indicators using the data breach incidents and operational control risk index are associated with an increased likelihood of future financial reporting control weaknesses, restatements and SEC comment letters, and increased audit fees.

One of the undetermined impacts of security breaches is the loss of trust from stakeholders. Prior literature suggests that firms provide more extensive risk factor disclosures to prepare against potential risks such as litigation or reputational loss (Campbell et *al.*, 2014). Managers expect a positive market reaction to more quantified risk disclosures around and after the filing dates (Filzen, 2015). Managers disclose their firms' cyber risks only when the cyber attack has a greater chance of upsetting the market reaction because withholding cyber risks is typically a more favorable choice for managers (Amir et *al.*, 2018).

To alleviate management discretion, Moody's, a rating agency, has developed a new set of cyber risk standards related to a firm's credit rating, thus providing a framework for managers to build up cyber defense mechanisms or respond to breach incidents (Fazzini, 2018). In short, investors have different sources of information to evaluate the impact of cyber attacks rather than just information provided by managers. Nevertheless, investors might rely on financial analyst reports as a good source of information.

3.1.2. The cybersecurity puzzle for financial analysts to solve

Despite the lack of credibility of the risk factor disclosures (Li et *al.*, 2018), investors do appear to find some merits in them as abnormal returns and future unexpected earnings around the filing dates are lower than before the dissemination of the risk disclosures. Filzen (2015) concludes that the SEC's requirements led firms to provide more timely disclosure of bad news. Filzen et *al.* (2016) find that firms with quarterly risk factor disclosure updates, including more direct words related to firm fundamentals, experience lower future abnormal returns than those without updates. These results suggest that, on average, markets react to such updates incompletely when the 10-Q is filed. The overall incompleteness is primarily driven by firms providing less specific disclosure about the effects of the risk on firm fundamentals. Analysts also tend to underreact to the same firms. In other words, selective or imprecise disclosures may reflect a lack of transparency about underlying risks.

Prior studies also discuss the advantages and disadvantages of firms sharing additional information about cybersecurity investments. According to Bodin et *al.* (2018), firms make more security investments to obtain favorable cyber insurance premiums or avoid relying on information sharing to reduce cybersecurity threats and cyber breach incidents. There is an optimal amount for each firm to spend on security investment to strengthen their cybersecurity depending on the types of potential cyber-attacks (Hausken, 2006; Tanaka et *al.*, 2005). Firms will only suffer small cyber losses if they invest appropriately in information security (Gordon et *al.*, 2002); however, evaluating their cyber vulnerabilities is challenging, given today's continuous innovations in digital technology.

Some studies also assess the benefits of information sharing for companies and society, such as improving cyber defense for firms willing to share their private information (Gordon et *al.*, 2003; Haapamäki et *al.*, 2019; Hausken, 2007). In this regard, Leung (2018) emphasizes that banks rely on information sharing to develop countermeasures following guidelines on preventing cyberattacks provided by the government and enforcement agencies. Hence, our study's focus on the bank industry allows us to leverage its information-sharing feature.

Despite being informative to financial users, details of cyber risk structure could provide a roadmap for malicious cyber-attacks. Additionally, cyber investments could attract unwanted attention from hackers who consider exploiting these strong cyber defenses challenging (Lesson et *al.*, 2005). Furthermore, hackers can exploit digital properties such as cloud migration without mandated security measures. According to Deloitte (2019), outsourcing, large-scale adoption of innovations, and machine learning pose significant cyber risks to U.S. banks since there are not yet specific regulations to control the quality of cybersecurity controls of those new features. As a result, cyber investments may increase the probability of cyber breaches within the banking industry. PwC (2018) emphasizes that leading financial institutions will continue their digital transformation and cost containment using artificial intelligence, advanced analytics, machine learning, and robotic process automation. Most mid-tier banks are currently in the process of digital transformation. Their partnership with outside vendors could, in turn, pose high cyber risks.

3.1.3. Financial analysts forecast properties of uncertainty or information asymmetry

Many elements also affect analysts' decisions to revise their earnings forecasts, such as information uncertainty among investors represented by analyst forecast dispersion (Zhang, 2006) or accounting restatements (Barniv et *al.*, 2009). According to Zhang (2006), analysts seem to underreact to information uncertainty among investors as the upward and downward forecast revisions are more significant when the information environment is more uncertain. In addition, a downward forecast revision is usually greater than an upward forecast revision due to the autocorrelation of bad news accumulated over time. Based on Zhang (2006), there are two sources of information uncertainty among investors: the quality of the information environment and the variability of a firm's fundamental value. Additionally, information uncertainty among investors implies that not all investors may accurately assess the firm's financial performance (Lu et al. 2010). On the other hand, some investors could have an advantage over others in identifying the firm's underlying value if they have access to proprietary data (Lu et al., 2010). Thus, the presence of private information underlies information asymmetries among investors.

Analysts also revise forecasts to get more accurate predictions and to enhance their career reputations. According to Stuerke (2005), the likelihood of analysts revising their forecasts depends heavily on their performance in the previous period. The distribution of information about corporate earnings via analyst forecast revisions facilitates the market price discovery process. Nevertheless, there is some debate about the usefulness of the information conveyed by analyst forecast revisions. Herding bias tends to occur when one analyst follows the analyst consensus forecast (Gleason et *al.*, 2004). Information searches by some skillful analysts and their subsequent market actions are more meaningful for investors than the simple revelation that analysts have revised their forecasts to follow the consensus forecast (Barniv et *al.*, 2009). Analysts forecast revisions following events such as restatement or earnings announcements or the initiation of coverage convey potentially helpful information to investors seeking to decipher the relevance and reliability of the underlying news.

This study investigates how analysts incorporate information about cyberattacks using the two components of analyst forecast dispersion: information asymmetry (information asymmetry among financial analysts) and uncertainty (information uncertainty among financial analysts) (Barron et al., 2009). Information asymmetry implies that a particular group may have a private information source that is unavailable to other investors. Limited access by financial analysts to information provided by top management increases information asymmetry. The absence of consensus among analysts quantifies it. Information uncertainty implies that not all analysts may accurately assess the firm's financial performance. The mean departure of analyst forecasts from reported earnings per share quantifies it. We presume that the limited access financial analysts have to information provided by top management increases information asymmetry. In addition, we consider uncertainty regarding idiosyncratic risk components related to the option value of the firm.

Prior studies also indicate a close relationship between uncertainty or asymmetry and analyst forecast accuracy (Barniv et *al.*, 2009; Gleason et *al.*, 2003; Lehavy et *al.*, 2011; Liu et *al.*, 2013; Stuerke, 2005). Based on Barniv et *al.* (2009), investors consider analyst forecast accuracy important for evaluating the quality of analyst forecast revision. Thus, while there is some overlap between uncertainty, information asymmetry, analyst forecast accuracy, and analyst forecast revision, these are four distinct yet related constructs. Gaining a broad understanding of how firm-specific events such as cyber incidents ultimately affect capital markets and investors requires that our analysis encompasses all four.

There are different factors affecting analyst forecast accuracy, such as transparency of financial information (Liu et *al.*, 2013), financial loss (Barniv et *al.*, 2009; Coen, Desfleurs, and L'Her, 2009), institutional ownership (Lehavy et *al.*, 2011) earnings volatility, number of analysts following (Hope, 2003), fair value accounting (Tan et *al.*, 2011) and financial leverage (Ayres et *al.*, 2017). A more transparent financial statement will help analysts reach more accurate forecasts (Yoon et *al.*, 2011). Firms with financial loss, higher earnings volatility, and higher financial leverage are more unpredictable and challenging for analysts to obtain accurate forecasts.

The higher the level of institutional ownership and the number of analysts following a particular firm, the more accurate the analyst forecasts due to the information searches of a more comprehensive set of players with incentives to gather better information. At the same time, according to Ettredge et *al.* (2018), higher institutional ownership and analyst coverage are associated with a higher probability of future breaches. Therefore, the probability of uncovering and disclosing security breaches is higher for firms due to tremendous pressure from analysts and institutional investors (Amir et *al.*, 2018), facilitating analysts' forecasting tasks.

Analyst forecast dispersion varies across firms according to the information asymmetry between firms and analysts and is closely related to uncertainty. As mentioned, Zhang (2006) uses analyst forecast dispersion as the proxy for uncertainty. The more uncertain the information environment, the more dispersed the analyst forecasts are and the longer it takes to update their forecasts. An uncertain information environment often leads to a negative association between analyst forecast dispersion and a future firm's return on investment (Barron et *al.*, 2009). Similarly, the greater the information processing cost, the more difficult analysts' forecast tasks and the higher the forecast dispersion is. Havakhor et *al.* (2020) emphasize the moderating role of financial analysts in encouraging firms to disclose cybersecurity investments to reduce uncertainty between firms and investors.

However, to reduce information asymmetry and analyst forecast dispersion, firms will provide more public disclosure of good and bad news via earnings announcements. According to Ali et *al.* (2019), analysts forecast dispersion increases when bad news about future earnings is released rather than good news. Firms usually withhold the disclosure of bad news to prevent adverse earnings shocks, leading to increased information asymmetry.

In prior studies, there are also many factors affecting analyst forecast dispersion, such as future stock returns (Ali et *al.*, 2019), information asymmetry (Lehavy et *al.*, 2011), market uncertainty (Barron et *al.*, 1998; Lehavy et *al.*, 2011), information processing cost (Lehavy et *al.* 2011) and earnings volatility (Liu et *al.*, 2012). Analysts find firms with negative future stock returns are more challenging to predict due to the delay in recognizing the negative effect of bad news (Ali et *al.*, 2019).

It may be more difficult for analysts to revise their forecast promptly to the release of damaging information such as cyber attacks. Managers are willing to hide cyber attacks if the probability of discovering them is low (Amir et *al.*, 2018), increasing uncertainty in an information environment. Hence, our study considers two significant elements influencing analyst forecast dispersion and accuracy: information asymmetry and uncertainty.

3.2. Hypothesis development

After the SEC 2011 cybersecurity guidance was released, some argued that cybersecurity disclosure was not useful to investors despite the positive market reaction to this new guidance (Berkman et *al.*, 2018). The full impact of cyberattacks is frequently unknown to the public, especially when cyberattack complexity is challenging to assess. This study examines how financial analysts perceive the consequences of various cyberattack types that range in the complexity of security breaches.

Analysts can distinguish between helpful information provided in firm disclosure and noise created by a firm's impression management strategy. They can also conduct extensive research to update their forecasts in response to the release of cyber attacks via multiple channels. Our study assumes that analysts can evaluate the cyber defense systems of organizations with security breaches despite the fact that firms are unwilling to share all the information regarding their security system in case of information leakage (Ettredge et *al.*, 2018) and exposure to security roadmaps (Higgs et *al.*, 2016). Each analyst has their investigation sources, and the frequency of their forecast updates relating to cyber attacks will vary depending on when cyber attacks become public information. The sooner they revise their earnings prediction, the higher the quality of the information environment investors will benefit from.

INSERT FIGURE 7 ABOUT HERE

According to Figure 6, we assume that the first notice date of cyber incidents is when banks reveal their breaches via various public channels, including 10K, 8K, press releases, and conference calls. Furthermore, analyst forecast revisions provide investors with helpful information for their decision-making, especially the quarterly analyst forecast revision (Gleason et *al.*, 2003). Therefore, our study states the first hypothesis as follows:

H1: Analysts are more inclined to adjust earnings forecasts for banks that experience cyber attacks than for banks that do not in the same quarter.

As banks attempt to reposition their business models through digital transformation, the impact of a security breach is likely to attract more attention from analysts as it may compromise a bank's future earnings. Moreover, analysts' considerations of their reputations may also force them to revise their earnings forecast. Stocks with high trading volumes and special events such as security breaches attract more interest from financial analysts, motivating them to revise their forecasts to earn more profits (Stuerke, 2005). As a result, we believe that cyber intrusions may prompt financial analysts to make a timely revision of their predictions.

In other words, financial analysts respond appropriately to the impact of cybersecurity breaches on the company's performance to reflect the true impacts of cyber attacks. The accident date, i.e., the actual date of cyber incidents, may not be publicly known, further increasing uncertainty about the cyberattack. The longer the gap between the date of the initial notice and the date of the accident, the fuzzier the information environment and the higher the risk of reputational damage and legal action for the banks. This study predicts that financial analysts will adjust their estimates of companies with security breaches over time to produce more accurate forecasts. The revised analyst forecasts will reduce the disparity in information between investors and their respective banks of interest.

Unknown is whether analysts choose to adjust their projections immediately or later. By examining the timeliness of the revision, this study aims to demonstrate if analysts have the urgency to respond rapidly to cybersecurity crisis events using their technical expertise. Before revising their earnings estimates, analysts may tend to await additional breach-related private information. Previous research has not examined the effects of hacks beyond market reaction. This study will explore the analyst report, which may be a tool for long-term investors. This study predicts that if the security breaches are significantly severe, financial analysts will need extra time to revise their earnings forecasts within the same timeframe that the bank breaches became public knowledge. Thus, the second hypothesis is the following:

H2: Analysts revise their quarterly earnings forecasts more slowly for banks that experience cyber attacks than for banks that do not in the same quarter.

Furthermore, financial damages caused by security breaches are published on social media and in news releases following security breaches. In contrast, reputation losses are more challenging to measure. The litigation procedure is lengthy for both plaintiffs and defendants in situations involving security breaches, and details regarding lawsuits are not made public. It could hamper analysts' estimate of the bank's future market value, resulting in a delay in modifying analyst earnings forecasts after a cyber attack becomes public knowledge. Past literature has not extensively examined the topic of litigation procedure. In addition, this delay may indicate that analysts may not execute their forecasting duty meticulously right after cyber attacks but rather wait until they have access to more reliable data.

For banks that experience cyber attacks, the longer the interval between the date of the first notice and the date of the event, the more ambiguous the information environment is, and the more serious the possible consequences of a cyber attack on a bank. As a result, analysts may have needed additional time to collect all relevant data before revising their earnings forecasts, as they deemed the severity of the intrusions to be substantial. During times of crisis, they may delay adjusting their forecasts out of an abundance of caution.

Too much information regarding cybersecurity procedures may jeopardize the banks' cyber security. Higgs et *al.* (2016) emphasize the positive relationship between the existence of a technology committee and the probability of cybersecurity breaches since there are more disclosures of cyber risks and controls in the firm with a technology committee. Some studies argue that hackers may be motivated to penetrate more challenging cybersecurity systems (Leeson and Coyne, 2005; Havakhor et *al.*, 2020). If cybersecurity rules are not implemented, analysts may find it challenging to examine the fundamental value of institutions in an unstable financial climate after cyber attacks, increasing uncertainty of forecasts for banks that suffer cyber attacks. In contrast, similar to our discussion in our case study (Chapter 2), financial analysts are more likely to apply more pressure on the top management of the banks to gather more private cyber information and to put a greater effort into improving the cyber information environment, thus reducing the uncertainty that underlies their earnings forecasts. Thus, the third hypothesis is as follows:

H3a: A cyber event is negatively associated with uncertainty among financial analysts in the banking industry.

Additionally, there are some doubts that managers have incentives to delay the public disclosure of negative cyber information unless the negative impacts of cyber breaches are recognized. According to Amir et al. (2018), when the possibility of detection is low, managers will downplay the existence of cyber attacks. In this regard, artificial intelligence (AI) is supposed to help mitigate data breach costs through the automation of security (IBM, 2022). According to IBM (2022), the average cost saving s for fully implementing security automation is $3.05 million. As more banks adopt AI to increase their productivity (e.g., through AI conversational banking) and improve their fraud detection and risk management, the probability of cybersecurity breaches can be mitigated for banks.[25] In addition, cloud computing is gaining popularity in the banking industry due to its advanced data analytics capabilities and resistance to hacking (provided that the process and supplier are well-regarded).[26] With a safer and more informative cybersecurity environment due to the adoption of artificial intelligence and cloud technology, the analyst may

[25] https://www.businessinsider.com/ai-in-banking-report

[26] https://www.mckinsey.com/industries/financial-services/our-insights/fast-forward-how-cloud-computing-could-transform-risk-management

be able to predict the likelihood of security breaches due to lower information asymmetry. Artificial intelligence and cloud technology could help top management of the banks predict future cyber breaches in a timely manner and mitigate data breach costs by providing proactive cybersecurity disclosure to financial analysts via quarterly earnings conference calls. Since our study focuses on the banking industry, we expect a negative correlation between cyber events and information asymmetry among financial analysts as two sides of the above arguments are reasonable for the banking industry.

H3b: A cyber event is negatively associated with information asymmetry among financial analysts in the banking industry.

The SEC lacked precise rules or material thresholds for the disclosure of cybersecurity risk management and incidents, thus allowing managers to potentially manipulate cybersecurity reporting and reducing the certainty among financial analysts toward the negative impacts of cybersecurity breaches in the banking industry. According to Amir et al. (2018), managers demonstrate a willingness to conceal occurrences of cyber attacks when the likelihood of detection is minimal. This behavior contributes to heightened levels of uncertainty within the information environment. There are two conflicting arguments about the impact of cyber breaches on financial analyst behaviors. As financial analysts have more uncertainty in their earnings forecasts for banks that have experienced cyber attacks, they may be reluctant to revise their earnings when the information environment is uncertain after cyber breaches. However, suppose financial analysts recognize the importance of the negative impacts of cyber breaches in the financial market. In that case, they may have an incentive to revise their earnings forecast to improve their career performance. With the pressure from financial analysts in our case study (second chapter) regarding the negative impacts of cyber breaches among five credit institutions, our study emphasizes the second argument in which there is a positive relationship between the likelihood of revision and uncertainty among financial analysts.

H4a: The likelihood of revision is positively associated with uncertainty among financial analysts in the banking industry.

Sell-side analysts' job in the secondary market is to investigate the reliability and accuracy of the information given by the managers, thus allowing them to provide proper analytical research for essential participants in the capital market, such as institutional investors and capital providers (Bradshaw et *al.*, 2017). According to Jung et al. (2018), the difference between sell-side and buy-side financial analysts is their accountability for stock recommendations. Institutional investment firms employ buy-side analysts and have a greater margin for error. In contrast, the sell-side analysts' compensation and employment security rely heavily on their stock recommendations. Some sell-side analysts might need to approach management via various channels about cybersecurity issues rarely highlighted in news releases or public disclosures before issuing their earnings forecast.

Additionally, the discussion between managers and sell-side analysts on conference calls provides them with important information, as illustrated in the previous chapter of this thesis. Simultaneously, it prevents bank managers from diverting attention from negative cybersecurity news and encourages them to disclose cybersecurity risks and controls via quarterly earnings conference calls under pressure by financial analysts, thus reducing information asymmetry among financial analysts. Low information asymmetry motivates financial analysts to increase their likelihood of earnings forecast revision to improve their career performance with less prediction risk. As a result, the following constitutes the fourth hypothesis:

H4b: The likelihood of revision is negatively associated with information asymmetry among financial analysts in the banking industry.

Overall, the relationship between the likelihood of revision and analyst forecast uncertainty and the relationship between the likelihood of revision and analyst information asymmetry are empirical questions to consider when evaluating the quality of financial analysts. Analysts' predictions become increasingly divergent because of the ambiguity of available information. Some financial analysts hesitate to revise their earnings forecasts when the quality of the information environment is low or uncertain. In contrast, others recognize the significant negative impacts of cyber breaches in their earnings forecast revision. Some experts may refrain from revising their forecasts quickly and instead wait patiently. In the event of a cyberattack, some analysts may believe there are chances for them to act in a manner that allows them to gain from the expanded availability of public information regarding cybersecurity risks and controls via quarterly earnings conference calls by making their earnings forecast revisions.

3.3. Data Sources and Sample Selection

Our study spans the period from 2007 to 2022. We focus on depository institutions (banks) to investigate the impact of cyber attacks on their requirement to meet specific statutory capital requirements and manage cash-related securities such as loans or deposits. The sample includes all 1,052 depository institutions (Commercial Banks, Savings Institutions, and Credit Unions with SIC 6000-6099) incorporated and headquartered in the U.S. for 37,311 quarterly observations. Financial data comes from quarterly Bank Compustat Fundamentals, quarterly stock return data from CRSP, and quarterly analyst forecasts and revisions from I/B/E/S Detail. Variables and data sources are specified in Appendix A.

Our study retrieves data on cybersecurity incidents from 2007 to 2022 from the Advisen database, which contains 1,110 cybersecurity incidents for U.S. depository institutions. Advisen collects economic loss from credible news outlets and by submitting Freedom of Information Act (FOIA) requests to states reporting these issues. For each event, the dataset contains details about the type of cyber event (e.g., data breach, cyber extortion, identity theft, phishing, spoofing, social engineering physical tampering, and privacy violation), type of firm, and industry (public or private, in industries such as finance, retail, and public administration), and extent of economic losses. The events are divided into three main categories: confidentiality, availability, and integrity.

We merge the depository institutions from Compustat and Advisen with all analyst earnings forecasts from IBES and stock return data from CRSP, yielding 78,300 analyst bank quarter observations (507 banks and 420 analysts). In this sample, 65 banks experienced at least one cyber incident between 2007 and 2022, while the remaining 442 did not. Table 1 provides further details about the filtering process used to construct the sample.

INSERT TABLE 1 ABOUT HERE

3.4. Research Method

Based on Huang et *al.* (2021), we conduct a propensity score matching analysis to examine whether the likelihood of revision, timeliness of earning forecast revision, forecast accuracy, forecast dispersion, uncertainty, and information asymmetry is significantly different between treatment (banks that suffer cyberattacks) and control (banks that do not suffer cyberattacks) groups. We use three sample sets for the analysis. The first sample set includes all analysts' earnings forecasts. The second sample set includes all updated analyst earnings forecasts. The third sample set is restricted to analyst earnings forecasts for cyberattacked banks.

In the first stage of the propensity score matching, we run a Probit regression with the dependent variable *TREATMENT* that is, in turn, each of the following indicator variables in the Appendix: *CYBER_EVENT, REVISE, SIZECAT, CYBGOV, CEOPOWER, SICREG, WELLCAP, NUMANACAT.* The model includes a set of explanatory variables for bank characteristics, specifically, *SIZE, BTM, LEV, NIM, ASSET TANGIBILITY, CAPR1Q, CAPR2Q, NPAT, PLL, NCO, STOCK_TURNOVER,* as well as two interaction variables *NIM x CAPR1Q, SIZE x NPAT* that capture. We also control individual financial analyst characteristics using the variables *NUMANA, EXPOSURE,* and *GENANA*. The full model is specified in Equation (1). The Probit model runs on all bank-quarter observations with available data from 2007 to 2022. The interaction between net interest margin and tier 1 capital regulatory ratio investigates whether banks attract interest from hackers due to the portfolio of profitability and risks. It is given that banks with high profitability tend to take more risks while banks with low profitability take fewer risks.

Additionally, the interaction between the size and non-performing total assets indicates whether small (large) banks with high (low) risk structures are more likely to experience cyber attacks. It is also given that big banks are more likely to take more risks while small banks take less risks. The purpose of these two interaction variables is to examine how the mix of three factors, such as profitability, size and risk structures of the banks, affect the probability of breaches within the banking industry, besides examining each factor separately. Our study investigates whether large banks with high-risk structures can implement efficient cyber defense systems or are more visible targets for cyber-criminals to increase their reputation in the black market.

We use propensity score matching with distinct sample sets for each hypothesis. We use 1 to 1 nearest neighbor propensity score matching by matching one control observation to one treatment observation to investigate the effect of cyber events or the likelihood of revision.

$TREATMENT = \alpha_0 + \alpha_1 BANK\ CHARACTERISTICS_t + \alpha_2 FINANCIAL\ ANALYST\ CHARACTERISTICS_t + \varepsilon\ (1)$

CYBER_EVENT is an indicator variable that equals one if banks experienced cybersecurity incidents such as malicious breach, physically lost or stolen data, unintentional disclosure, information technology processing errors, identity fraud, network or website disruption, phishing, or privacy violation in quarter *t*, and zero otherwise. We use the obtained coefficients to estimate the propensity score for distinct sample sets. We then use the Probit propensity score to construct matched samples of bank-quarter observations that, ex-ante, have the same probability of suffering a cyber event.

Next, we explain the explanatory variables included in the Probit model. *SIZE* is the natural log of total assets expressed as a quarter *t* value. Larger banks are more susceptible to cyber attacks because they contain more sensitive client data and intellectual property, attracting the interest of financial analysts. Analysts may view size as essential in determining the impact of cyber incidents on banks' earnings per share predictions for the upcoming quarters. Larger banks are more likely to suffer reputation damage due to cybersecurity problems.

Similarly, banks with high net interest margin (*NIM*) value in quarter *t* may be prime targets for cybercrime. Analysts may also evaluate a bank's ability to respond to cybersecurity breaches' financial and social consequences based on the net interest margin it generates in each quarter.

Banks with a higher book-to-market value (*BTM*) in the quarter *t* can better guard against cyber crime in times of crisis. Banks with an immense book-to-market value (*BTM*) in a quarter have a greater capacity to defend against cybercrime in times of crisis and are therefore rated highly by analysts.

ASSET TANGIBILITY is estimated as the ratio of quarterly gross property, plant, and equipment to total quarterly assets during quarter *t*. *ASSET TANGIBILITY* is a valuable indicator of a bank's essential infrastructure; however, cloud computing and mobile platforms may render it less relevant than in the past. *LEV* equals the quarterly short- and long-term debt ratio to the market value of common equity in quarter *t*. A bank's structure of risk-weighted assets typically results in a high leverage ratio.

Capital regulation ratios based on Basel III capital requirements[27] are often used to evaluate the likelihood that banks are in a financial meltdown. Tier 1 capital (*CAPR1Q*) must be at least 6%, and Tier 2 capital (*CAPR2Q*) must be at least 2% to cover risk-weighted assets following Basel III capital regulations. In other words, regulatory capital ratios are a requirement for bank capital sufficiency, stress testing, and liquidity needs.

Other control variables, such as total nonperforming assets (*NPAT*), provision for loan losses (*PLL),* and net charge-off (*NCO*), indicate the recording and management of bank client defaults during a crisis. The study also includes some interaction terms, *NIM x CAPR1Q* and *SIZE x NPAT,* to emphasize the overall effect of banks' capability to respond to cyber crises despite having the risk of loan defaults.

Another control variable *STOCK_TURNOVER* is the number of shares traded in quarter *t* divided by the firm's average number of shares outstanding in quarter *t* for firm *i*. This variable is used to indicate market reaction from investors. *NUMANA,* which refers to the natural log of the total number of analysts following the banks during quarter *t*, is the control variable for individual

[27] https://www.bis.org/basel_framework/chapter/RBC/20.htm?inforce=20191215&published=20191215

bank earnings forecasts. On the other hand, *GENANA* is a natural log of the number of quarters between the analyst *j*'s first forecast in IBES and her current forecast at quarter *t*. At the same time, *EXPOSURE* is a natural log of the financial analysts' number of quarters covering the bank. The broad experience and exposure to a bank over multiple quarters will be good indicators of the quality of financial analysts' revision forecasts.

3.4.1. Model specification to test the relation between cyber events and individual analyst earnings forecast for all earnings forecasts

We conduct statistical tests for the first hypothesis using propensity score matching to estimate the relationship between the likelihood of forecast revision and the bank cyber attack for the first hypothesis. In this case, we will examine all the individual analyst earnings forecasts from 2007 to 2022, including the analysts who do not revise their forecasts and those who revise their forecasts after cyber attacks. *CYBER EVENT* is the treatment effect of this regression model. We compare the analyst forecast revision for the banks that suffer cyber attacks with banks that do not suffer cyber attacks:

$$REVISE_t = \alpha_0 + \alpha_1 CYBER\_EVENT_t + \alpha_2 BANK\ CHARACTERISTICS_t + \alpha_3 FINANCIAL\ ANALYST\ CHARACTERISTICS_t + \varepsilon \quad (2)$$

This first regression model examines the first hypothesis in which we investigate whether cyber attacks influence the financial analyst's decision to revise their forecast. On the other hand, the second regression model will use only the analysts who revised their forecasts to identify whether these financial analysts can identify the impact of cyber attacks by estimating the financial analyst forecast properties.

Then we use propensity score matching with the treatment effect *CYBER_EVENT,* capturing the impact of cybercrime activities on *ANALYSTS EARNINGS PROPERTIES* such as analyst forecast accuracy (*FERROR)*, forecast dispersion *(DISP)*, uncertainty (*UNCERTAINTY),* and information asymmetry (*INFORMATION ASYMMETRY)* using the following regression models:

$ANALYSTS\ EARNINGS\ PROPERTIES_t = \alpha_0 + \alpha_1 CYBER\_EVENT_t + \alpha_2 BANK\ CHARACTERISTICS_t + \alpha_3 FINANCIAL\ ANALYST\ CHARACTERTICS_t + \varepsilon$ *(3)*

FERROR is the absolute difference between the most recent analysts' projections and the actual earnings per share of the company, scaled by stock prices for the same quarter. It is unclear whether analysts choose to obtain more accurate forecasts for the banks they follow based on the bank's conditions or capabilities. In addition, cybersecurity threats may cause analysts' earnings forecast errors to decrease over time due to unavailable cyber breaches of private information. However, banks with a more remarkable ability to respond to the breach (higher regulatory capital ratios and a lower likelihood of loan defaults) may attract more analysts' attention, resulting in less forecast error.

DISP is the analyst forecast dispersion, calculated as the standard deviation of analysts' earnings per share (EPS) projections scaled by various analysts' absolute value of the mean EPS for the same quarter. This dependent variable measures the deviation of individual analyst forecasts from the consensus. Although the earnings forecast dispersion consists of two fundamental components (uncertainty and information asymmetry), it is unknown whether the dispersion varies owing to information asymmetry or uncertainty (Barron et *al.*, 2009). *FERROR* and *DISP* are trimmed by one percentage to control for outliers in the data.

Inadequate private breach information or uncertain cybersecurity risks and controls during cyber breach events might lead to conflicting analyst opinions regarding bank victims of cyber attacks. Thus, this study also investigates the dynamics of information asymmetry and uncertainty following cyber attacks. According to Barron et *al.* (2009), *UNCERTAINTY* is measured as the mean departure from reported earnings per share. In contrast, the absence of consensus among financial analysts quantifies *INFORMATION ASYMMETRY*. The estimations for these two variables are as follows:

UNCERTAINTY = $\left(1-\frac{1}{n}\right)D+SE$ (4)

INFORMATION ASYMMETRY = $\frac{SE-D/n}{\left(1-\frac{1}{n}\right)D+SE}$ (5)

(D: forecast dispersion, that is, the sample variance of the individual forecast around the mean forecast; SE: squared error in the mean forecast, measured as the difference between earnings per share and the mean forecast; n: the number of individual forecasts)

Based on prior studies by Barron et al. (1998) and Barron et al. (2009), the individual analyst forecast dispersion around the average forecasts provides insights into the presence of information asymmetry while inaccuracies in the average forecasts provide clarity regarding the common uncertainty. This study investigates whether financial analysts' properties, such as information asymmetry and uncertainty, can reflect how financial analysts incorporate information regarding cyber breaches.

3.4.2. Model specification to test the relation between cyber events and individual analyst earnings forecast for the analysts who choose to revise their forecasts

First, we use propensity score matching with the treatment effect *CYBER EVENT* using the new sample set, which only includes analyst earnings forecast revision to investigate the effect of severity of a bank cyber attack on the timeliness of earnings forecast revision with the accident or the first notice date discovered by the public:

$DELAY\ OF\ REVISION_t = = \alpha_0 + \alpha_1 CYBER\_EVENT_t + \alpha_2 BANK\ CHARACTERISTICS_t + \alpha_3 FINANCIAL\ ANALYST\ CHARACTERTICS_t + \varepsilon$ *(6)*

The number of days between the date of the most current analyst earnings forecast and the date of the last analyst earnings forecast revision for quarter *t* is the *DELAY OF REVISION*. In other words, the longer time between updates demonstrates the analyst's reluctance to adjust their forecasts in light of actual occurrences. Surprisingly, some analysts have chosen to revise their forecast a few times until they are satisfied with the final forecast revision according to the IBES database.

The uncertainty or asymmetry substantially affects the timeliness of analyst prediction adjustment when comparing banks with cybersecurity breaches to those without in recent years. This ambiguity or asymmetry is illustrated by the banks' financial conditions (*BTM, LEV, and NIM*) and their ability to respond to breaches *(CAPR1Q, CAPR2Q).*

In addition, banks with more intangible assets, such as digital platform systems, are more susceptible to cybercrime and may exacerbate the information asymmetry between banks and the public. Additionally, revision timeliness is contingent upon the analysts' financial capabilities, measured by general and specific experience with the banking industry (*GENANA and*

EXPOSURE). The number of shares (*STOCK TURNOVER*) traded in the market might affect analysts' decision to revise their forecast more correspondingly.

Finally, we also investigate the earnings forecast accuracy and dispersion along with uncertainty and asymmetry among the individual analysts who chose to revise their forecasts to examine whether revised forecasts for banks that suffer cyber attacks are necessarily better than those for banks that do not suffer cyber attacks by using a new sample set for the regression model (2) and (3).

3.4.3. Model specification to test the relation between cyber events and individual analyst earnings forecast for the analysts who issue forecasts for banks that suffer cyber attacks

We use propensity score matching with the treatment effect *REVISE* and limit the sample to only banks that suffer cyberattacks to study how the likelihood of revision is related to different types of cyberattacks, earnings forecast dispersion, uncertainty, or asymmetry. Besides the previous bank characteristics, our study also includes variables that capture the type of the cyber event (*CONFIDENTIALITY, AVAILABILITY, INTEGRITY)* and financial damage (*DAMAGE and AFFECTED_COUNT)* due to cyber attacks for each of the banks we examine in the following regression models:

$ANALYSTS\ EARNINGS\ PROPERTIES_t = \alpha_0 + \alpha_1 REVISE_t + \alpha_2 CYBER\_EVENT\ TYPE_t + \alpha_3 FINANCIAL\ DAMAGE_t + \alpha_4 BANK\ CHARACTERISTICS_t + \alpha_5 FINANCIAL\ ANALYST\ CHARACTERTICS_t + \varepsilon\ (7)$

Some new variables, such as *CONFIDENTIALITY, AVAILABILITY, and INTEGRITY*, are added*,* indicating different types of cyber attacks. Based on the Advisen database, cyber events related to confidentiality include “Data - Physical Lost or Stolen,” "Data - Unintentional

Disclosure," "Data - Malicious Breach," "Privacy - Unauthorized Contact or Disclosure" and "Privacy – Unauthorized Data Collection." Illegal use of confidential information, such as credit card numbers and other personal data, illustrates a breach of confidentiality. Accordingly, it is prudent to anticipate that this type of breach can potentially cause severe long-term harm to the reputation of a business, including the loss of trust among consumers (Zafar et *al.*, 2016).

Cyber events related to availability include "Network/Website Disruption" and "Cyber Extortion." The prevention of computer or network failures and malicious data denials is a prime example of availability. It has fewer chances to harm the company's and its clientele's connection over time (Zafar et *al.*, 2016). Three remaining case types, including "Phishing, Spoofing, Social engineering," "Skimming, Physical Tampering," and "Identity - Fraudulent Use/Account Access," will be put into the Integrity category. *DAMAGE* is the dollar damage estimated for the attacked firm scaled by the firm's market value of equity. *AFFECTED_COUNT* is the number of records exposed during the breach in quarter *t*. Those two variables are added to control the severity of cyber attacks. According to Zafar et *al.* (2016), the integrity-related breach is illustrated by web page alteration and data tampering caused by computer malware. It is unlikely to permanently harm the company's credibility, as data corruption can be quickly resolved.

3.5. Results

3.5.1. Descriptive statistics

Table 2 provides details about the three sample sets that are used in this study, i.e., banks with individual analyst earnings forecast data (76,750 observations), banks with individual analysts who revise their forecast (26,062 observations), and banks with individual analysts who issue forecasts for banks that experience cyber attacks (6,183 observations). The sample essentially comprises large banks across the United States.

INSERT TABLE 2 ABOUT HERE

The correlation statistics in Panel A of Table 3 indicate that the likelihood of revision is positively associated with cyber breaches (the correlation between *REVISE* and *CYBER_EVENT: 0.137*). Additionally, negative correlations exist between *CYBER_EVENT* and individual analyst forecast error (*FERROR: -0.045*) and earnings forecast dispersion (*DISP: -0.021*). According to Panel A, the level of uncertainty is not significantly related to cyber breaches (*UNCERTAINTY: 0.002*). In contrast, the level of information asymmetry is lower for banks that experienced security breaches (*INFORMATION ASYMMETRY: -0.119)*. In addition, banks that have good cybersecurity governance or a more robust top management CEO tend to attract more interest from hackers as their probability of breaches is higher (*CYBGOV: 0.209; CEOPOWER: 0.083*). Similarly, federally supervised banks (*SICREG: 0.037*) or banks with the high number of analysts following (*NUMANACAT: 0.26*) have experienced more cyber breaches. Finally, banks with high capital reserves also have more cyber attacks (*WELLCAP: 0.028*).

The bivariate correlations in panel B of Table 3 show that cyber breaches are positively related to the delay of revision (*DELAY_OF_REVISION: 0.049*). Cyber breaches are negatively associated with uncertainty (*UNCERTAINTY: -0.011*) and information asymmetry (*INFORMATION ASYMMETRY: -0.112*) among financial analysts.

Based on the bivariate statistics in Panel C of Table 3, financial analysts are more likely to revise their forecasts for *INTEGRITY* cyber breaches (*-0.027*) while they are indifferent toward their forecast for *CONFIDENTIALITY* (*0.014*) and *AVAILABILITY* (*-0.023*) cyber breaches.

Moreover, the likelihood of forecast revision is positively associated with uncertainty (*UNCERTAINTY: 0.117*) and negatively associated with information asymmetry (*INFORMATION ASYMMETRY: -0.131*) among financial analysts.

INSERT TABLE 3 ABOUT HERE

3.5.2. Main Results

Table 4 shows the results from the analysis of the relation between the occurrence of cyber events and individual analyst earnings forecast data. Individual analyst forecasts for banks that experienced a cyber event are matched with those for banks that did not experience such an event using propensity score matching. Panel A of Table 4 presents the results from the first stage of Probit analysis on the determinants of cyber events. It appears that banks are more likely to experience a cyber event if they are larger *(SIZE: 0.572; p < 0.01*), have larger book-to-market ratio (*BTM: 0.079; p < 0.01*), lower profit margin (*NIM: -9 .672; p < 0.01*), larger asset tangibility (*ASSET_TANGIBILITY*: *14.1; p < 0.01*), lower tier 1 capital (*CAPR1Q: -0.035; p < 0.01*), more non-performing total assets (*NPAT: 7.636; p < 0.10*), lower provisions for loan losses (*PLL: -57.373; p < 0.01*) and are followed by more analysts *(NUMANA: 0.171; p < 0.01*). Based on the results above, our study implies that large banks with higher risk structures are more likely to experience cyber attacks. We can assume that hackers have more financial gain from penetrating these banks' cyber defense. Provision for loan losses indicates the number of banks' future default loans that management predicts. In contrast, non-performing total assets indicate the current default loans as the banks' customers fail to make principal and interest payments for the specific period. Therefore, lower loan loss provisions and higher nonperforming total assets reflect the higher risk structure taken by the top management of these banks.

Panel B of Table 4 shows the results of second-stage regressions relying on PSM for the relation between the occurrence of a cyber event (*CYBER EVENT (1 vs. 0)*) and analysts' forecast errors (*FERROR*), analyst forecast dispersion (*DISP*), analyst forecast revision (*REVISE*), uncertainty (*UNCERTAINTY*) and information asymmetry (*INFORMATION ASYMMETRY*). Results in column 3 of the table show that the occurrence of a cyber event in a bank (*CYBER_EVENT*) increases the likelihood of a forecast revision (*0.071; $p < 0.01$*), which is consistent with the first hypothesis.

Moreover, results in column 1 indicate that the occurrence of a cyber event (*CYBER EVENT)* in a bank does not significantly affect forecast errors but does lead to a reduction in analyst forecast dispersion (*-0.018; $p < 0.01$*), reduces uncertainty (*-0.356; $p < 0.01$*) but does increase information asymmetry (*0.038; $p < 0.01$*).

INSERT TABLE 4 ABOUT HERE

3.5.3. Analyst forecast revisions and information environment

This section focuses on financial analysts who decide to make earnings forecast revisions following a cyber event and how it affects uncertainty and asymmetry. Panel A of Table 5 presents the results of the first stage of probit regression on the determinants of the likelihood that a bank will experience a cyber event for the sample of banks with forecast revisions by analysts. Results from the first stage match those reported for panel A of Table 5. In Panel A of Table 5, the results show that financial analysts are more likely to revise their forecasts for larger banks exhibiting features of a stable financial condition to face cyber events. Additionally, analysts are more likely to revise their forecast for banks with more significant overall risks based on high covenants and big banks' reputations, which profit-seeking cybercriminals might target.

Panel B of Table 5 presents the results of the second-stage regressions for various analyst information properties when analysts revise their forecasts. As shown in column 1, banks experiencing a cyber event (*CYBER EVENT* (1 vs. 0)) exhibit a lower forecast error (*FERROR*) following the revision by an analyst (*-0.0013; p < 0.01*).

Moreover, results in column 4 show that banks experiencing a cyber event exhibit less uncertainty (*-0.928; p < 0.01*) following a forecast revision. It may imply that financial analysts put more effort into collecting information and generating better earnings forecasts for banks that suffered cyber attacks, thus improving the quality of the information environment and reducing uncertainty. It conflicts with the third hypothesis, in which we expect a positive relationship between a cyber event and uncertainty, as the quality of the cyber information environment might be negatively affected without the involvement of financial analysts.

However, for banks having experienced a cyber event followed by a forecast revision, there is no relation with *DISP, DELAY OF REVISION, or INFORMATION ASYMMETRY* (all coefficients have *p > 0.10*). As a result, cyber events are not associated with forecast dispersion, delay of revision, or information asymmetry. According to column 2, financial analysts have similar forecast behavior between banks that suffer cyber attacks and banks that do not, as the analyst forecast dispersion is not different between banks that experienced cyber breaches and banks that did not.

Moreover, cyber breaches did not force financial analysts to be under pressure to revise the earnings forecast more quickly. The results in column 3 show that financial analysts did not necessarily take longer to revise their forecast due to cyber breaches. Financial analysts' delay in revision relied on factors other than cyber breaches. As a result, the second null hypothesis is valid. We also expected that financial analysts did not have similar forecasts due to the uncertain cyber information environment after security breaches. The result in column 5 indicates that the third null hypothesis is valid. A cyber event is not associated with information asymmetry among the financial analysts who chose to revise their forecasts.

INSERT TABLE 5 ABOUT HERE

3.5.4. Analyst forecast properties and cyber events

For the fourth hypothesis, the research investigates the relationship between likelihood revision and earnings forecast error, earnings forecast dispersion, uncertainty, and information asymmetry. Panel A of Table 6 presents the first stage of the PSM analysis to identify the determinants underlying analysts' decision to revise their forecast (*REVISE*) (column 1). Until now, most reported cyber incidents have been *CONFIDENTIALITY* breaches, such as data breaches and privacy violations. However, other types of cyber incidents can also occur. Frequent *AVAILABILITY* breaches throughout the years may make it difficult for financial analysts to collect data promptly to release earnings forecasts. In contrast, *INTEGRITY* incidents occur infrequently and cause uncertain reputational harm to banks. Thus, we include control variables for the incident type to ascertain its potential impact on the likelihood of a forecast revision.

According to panel A of Table 6, it appears that analysts are more likely to revise their forecast for banks with a larger size (*SIZE: 0.32; p < 0.01*), more excellent book-to-market ratio (*BTM*: 0.646; p < 0.01), greater leverage (*LEV: 0.405; p < 0.05*), higher profit margin (*NIM: 5.814; p < 0.05*), less non-performing loans (*NPAT: -11.42; p < 0.01*), higher provisions for loan losses (*PLL: 47.376; p < 0.01*).

Panel A of Table 6 also shows a negative correlation between *DAMAGE (-0.0005; p< 0.05*) and the likelihood of revision (*REVISE*). Therefore, we can conclude that financial analysts are reluctant to revise forecasts for banks that have experienced more severe cyber damage. Additionally, there is a negative relationship between the likelihood of revision (*REVISE*) and *STOCK TURNOVER* (*-0.24; p < 0.01*). Financial analysts are also less likely to revise their forecasts for banks experiencing higher trading volumes.

According to Panel A of Table 6, financial analysts are less likely to revise their earnings forecasts for banks that experience *CONFIDENTIALITY* breaches because of a volatile cyber information environment due to heavy pressure from the public partly expressed in the press release (*-0.133; p < 0.10*). Understandably, *AVAILABILITY* and *INTEGRITY* cyber incidents do not affect the likelihood of revision, given their presumed insignificance.

Panel B of Table 6 presents results from the second stage of propensity score matching with *REVISE* as the treatment. This panel explores the relationship between the likelihood of revision and earnings forecast error, dispersion, uncertainty, and information asymmetry. The revision of a forecast by analysts ((*REVISE* (1 vs. 0)) does not translate into a difference in the forecast error between the financial analysts who choose to revise forecasts and those who do not (*column 1: 0.0004; p > 0.1*) but does lead to increased forecast dispersion (*column 2: 0.036; p < 0.01*), greater uncertainty (*column 3: 0.453; p < 0.01*) and less information asymmetry (*column 4: -0.025; p < 0.05*).

Furthermore, after running statistical tests on separate dependent variables *FERROR, UNCERTAINTY*, and *INFORMATION ASYMMETRY* for the matched samples, it appears that analysts made fewer earnings forecast errors for banks that suffer integrity-related cyber breaches (*INTEGRITY: -0.0008; p < 0.01*) while higher earnings forecast errors for banks which suffer availability-related breaches (*AVAILABILITY: 0.0008; p<0.1*) according to Column 1 of Panel B. Earnings forecast errors for confidentiality-related (*CONFIDENTIALITY: 0.0002; p>0.01*) are more unpredictable as some analysts generated more forecast errors while others did less. The indirect costs of confidentiality-related cyber breaches are challenging for financial analysts to measure. The indirect costs of confidentiality-related cyber breaches require financial analysts to collect information regarding the estimated loss of business and post-breach costs. On the other hand, financial analysts struggle to incorporate minor damages from frequent availability-related cyber issues, usually two or three times a year, into the financial valuation model, resulting in higher earnings forecast errors for banks that suffer availability-related cyber attacks.

Lower *DISP* in Column 2 (*CONFIDENTIALITY: -0.042; p<0.01*) and lower UNCERTAINTY in Column 3 (*CONFIDENTIALITY: -0.569; p<0.01*) for confidentiality-related cyber breaches indicate great efforts made by financial analysts to improve the quality of the information environment. Similarly, there is negative *DISP* in Column 2 *(INTEGRITY: -0.042; p<0.01*) and negative *UNCERTAINTY* in Column 3 (*INTEGRITY: -0.571; p<0.01*) for integrity-related cyber breaches. It indicates similar responses from financial analysts due to public pressure. The *DISP* for availability-related (*AVAILABILITY: -0.017; p>0.1*) and integrity-related cyber breaches (*INTEGRITY: -0.02*) are not significant, according to column 2. However, the *UNCERTAINTY* among the earnings forecast is lower for integrity-related issues (*INTEGRITY: -1.044; p<0.01*), according to column 3, indicating that financial analysts put more effort into enhancing the information environment and reducing uncertainty.

While the information asymmetry for confidentiality-related cyber breaches decreases (*CONFIDENTIALITY: -0.027; p<0.01*), the information asymmetry for integrity-related (*INTEGRITY: 0.137; p<0.01*) and availability cyber breaches (*AVAILABILITY: 0.157; p<0.01*) in Column 4 increases. Based on the above information, financial analysts are more likely to enhance the information environment by providing more detailed earnings forecasts for banks that suffer confidentiality-related cyber attacks, reducing the overall information asymmetry. In contrast, financial analysts find it difficult to reach a consensus forecast due to uncertain cyber management practices for integrity-related and availability-related cyber breaches during a cyber crisis.

INSERT TABLE 6 ABOUT HERE

3.6. Summary and Discussion

According to Panel A of Table 4, larger banks with lower loan quality and more performance issues are more likely to face cyber events. One can infer that larger banks hold more sensitive client data and intellectual property, making them more likely to be targeted by cybercriminals, especially if their financial condition suggests that they may not be making the necessary investments in cybersecurity. Hackers may target larger banks to improve their standing on the black market. Additionally, banks, such as Bank of America or Bank of New York Mellon, invest a lot in data centers and digital infrastructure nowadays, making these banks more vulnerable to cyber breaches. Banks with higher risks of loan defaults might have poor cybersecurity controls and higher cyber risks.

Consistent with the first hypothesis, financial analysts are more willing to revise their forecast for banks with cyber attacks than those without. However, financial analysts do not treat the banks that suffer cyber attacks differently from other banks when constructing their earnings valuation, as there are no differences in analyst forecast errors based on Table 4 (Panel B) column 1. The corresponding reductions in earnings forecast dispersion and uncertainty among financial analysts in columns 2 and 4 of Table 4 suggest the potential for some herding behavior among analysts following cyber events.

The second hypothesis is that analysts revise their quarterly earnings forecast more slowly for banks that experience cyber attacks than for banks that do not in the same quarter. According to column 3 of table 5 (Panel B), some financial analysts revise the earnings forecast quickly while others do not, as the coefficient for Cyber Event is insignificant. Also, analysts who revise their forecast for banks that experience cyber attacks exhibit lower earnings forecast errors than for banks that do not experience cyber attacks based on column 1 of Table 5 (Panel B).

The first part of the third hypothesis is that a cyber event is negatively associated with uncertainty among financial analysts in the banking industry. Analyst forecast dispersion reflects both uncertainty and information asymmetry among financial analysts. According to column 2 of table 4 (Panel B), the reduction in analyst forecast dispersion signals that uncertainty's positive impact is more significant than information asymmetry's negative impact. Furthermore, according to column 4 of Table 4 (Panel B), financial analysts exhibit less uncertainty for banks that suffer cyber attacks than for others due to greater efforts made to improve their forecast quality and information environment despite the argument that the unpredictability of information environment after cyber breaches might increase uncertainty. The negative association between the occurrence of a cyber event in a bank and uncertainty is consistent with the third hypothesis.

Despite our assumption that artificial intelligence and cloud technology help top management predict the probability of breaches, the positive coefficient of *CYBER EVENT* in column 4 of Table 4 (Panel B) shows that we underestimate the negative impacts of cyber breaches on the information environment. As top management provides limited private information about cyber risks and controls to the public, the results show that cyber information asymmetry is high, which contradicts the second part of the third hypothesis. The conflicting results between information asymmetry and uncertainty are consistent with a previous study. Prior research by

Barron et al. (2009) indicates that analysts forecast dispersion levels provide valuable insights into the uncertainty surrounding the company's prospects. However, changes in analyst forecast dispersion serve as signals for changes in information asymmetry. They emphasize a negative correlation between uncertainty and future stock returns, although a positive correlation is shown between information asymmetry and future stock returns.

INSERT FIGURE 8 ABOUT HERE

Financial analysts revise their forecasts to improve their reputation in the financial market, especially after cyber breaches. Table 5 focuses on the difference between the revision forecast for banks that suffer cyber attacks and banks that do not. After conducting the cross-sectional statistical test for only financial analysts who revised their earnings forecast, we obtained results similar to those reported in Table 4. Financial analysts who chose to revise forecasts experience less uncertainty for banks that suffer cyber attacks than for others. The lower uncertainty among financial analysts is consistent with the third hypothesis, reflecting that cyber events induce lower uncertainty among analysts with respect to their earnings forecasts. In other words, financial analysts put more effort into revising their forecasts for banks that experience cyber attacks than for banks that do not.

The first part of the fourth hypothesis is that the likelihood of revision is positively associated with uncertainty among financial analysts in the banking industry. This hypothesis looks only at the banks that suffered cyberattacks and identifies how financial analysts react toward different cyber events. Consistent with the first part of the hypothesis, the positive coefficient of *REVISE* in column 3 of Panel B of Table 6 indicates that financial analysts are more likely to revise their earnings forecasts when they recognize the opportunity to improve their career performance. Despite the efforts made by those financial analysts to revise forecasts after cyber breaches, they did not necessarily do a better job than financial analysts who decided to stay put after cyber breaches based on the coefficient of *REVISE* in column 1 of Table 6 (Panel B). However, when there is more uncertainty among their earnings forecasts, skillful analysts can still benefit from revising their earnings forecasts, which might explain the positive relationship between uncertainty and the likelihood of revision.

The results in column 2 of Table 6 (Panel B) indicate that analysts' forecast dispersion is higher following a cyber attack. Hence, uncertainty's positive impacts are larger than information asymmetry's negative impacts. These results indicate that financial analysts find it difficult to reach similar forecasts for banks that experience cyber attacks. According to the negative coefficient of *REVISE* in column 4 of Table 6 (Panel B), low information asymmetry reduces the forecasting risks and encourages financial analysts to revise their earnings forecasts more frequently to enhance their career performance. We can also conclude that financial analysts are reluctant to revise their earnings forecast when the information asymmetry is high due to limited private cyber information. Once again, there are conflicting results between the uncertainty and information asymmetry among financial analysts forecasting the banks that have experienced cyber attacks.

Based on the coefficients in Table 6 for three distinct types of cyber events, we can conclude that there is less uncertainty around banks that experience confidentiality-related breaches and integrity-related breaches due to the greater efforts made by financial analysts to recognize the significant impact of these types of breaches. It is expected that analysts have less information asymmetry regarding banks that have suffered breaches of confidentiality, given that such information is readily available in online newspapers. While availability-related breaches occur frequently and predictably, integrity-related breaches are rare and unpredictable. Analysts believe these two types of data breaches contain more confidential data that is difficult to discover.

3.7. Additional Analyses

Additional cross-sectional tests are performed to understand better factors that may underlie Table 4's results. For these tests, the overall sample is split into different subsample sets. The factors include bank size, cybersecurity governance, CEO power, regulatory oversight, regulatory capital ratios, and the number of analysts following.

First, using the mean average bank size, our study splits the sample into two subsamples. This additional analysis aims to separate the impacts of *NUMANA* (number of analysts) and *SIZE* as their correlation in Table 3 (Panel A) is 0.817. Our study uses *SIZECAT* as the indicator variable, which equals 1 if the bank size is above the overall sample average or 0 otherwise. Panel A of Table 5 presents the results from the first stage of probit analysis with *SIZECAT* as the treatment effect and *CYBER_EVENT* as the main independent variable alongside the other explanatory variables from Equation (1). The results show that attacked banks are more likely to be large (*CYBER_EVENT: 0.706; p<0.01*). Hackers are more motivated to exploit large banks for more monetary awards and increase their fame in the black market.

Furthermore, column 3 and 4 of Panel B of Table 7 indicates that *UNCERTAINTY* is larger for large banks (*SIZECAT*: *0.939; p<0.01*) while *INFORMATION_ASYMMETRY* is lower for large banks than for small banks (*SIZECAT: -0.053; p<0.01*).

INSERT TABLE 7 ABOUT HERE

Second, our study splits the sample into two subsamples using the *CYBGOV* as the indicator variable equal to 1 if the bank's top management team has a CIO, Chief Security Officer (CSO), Chief Security Information Officer (CSIO), Chief Privacy Officer (CPO), Chief Risk Officer (CRO), VP of Information, Director of IT, or IT Director during the fiscal year, or 0 otherwise. Panel A of Table 6 presents the results from the first stage of probit analysis with *CYBGOV* as the treatment effect and *CYBER_EVENT* as the independent variable. The results show that cybersecurity governance is unrelated to cyber events (*CYBER_EVENT: -0.027; p>0.1*). It is uncertain whether good cybersecurity governance would reduce the probability of cyber breaches. There is also an argument that banks with a higher probability of cyber breaches are more likely to hire top managers with more cyber expertise.

INSERT TABLE 8 ABOUT HERE

According to columns 3 and 4 of Panel B Table 8, good cybersecurity governance increases *UNCERTAINTY (CYBGOV:0.224; p<0.01*) and decreases *INFORMATION_ASYMMETRY (CYBGOV: -0.021; p<0.01*). This result is similar to the results in Table 7. Financial analysts have different opinions regarding their predictions for large banks or banks with good cybersecurity governance. However, they are motivated to enhance the overall information environment for these banks.

Third, the sample is split into two subsamples using the *CEOPOWER* as the indicator variable equal to 1 if the bank's CEO is also chairman or 0 otherwise.

INSERT TABLE 9 ABOUT HERE

Panel A of Table 9 presents the results from the first stage of probit analysis with *CEOPOWER* as the treatment effect and *CYBER_EVENT* as the independent variable. The results show that CEO duality is inversely related to cyber events (*CYBER_EVENT: -0.272; p<0.1*). CEO duality helps improve the banks' IT security to prevent future cyber events as the CEO has more power to implement the appropriate cybersecurity controls and hire cyber security talents.

According to columns 3 and 4 of Panel B Table 9, CEO duality decreases *UNCERTAINTY (CEOPOWER: -0.633; p<0.01*) and increases *INFORMATION_ASYMMETRY (CEOPOWER:*

0.025; p<0.01). Financial analysts reach similar forecasts toward banks with CEO duality but find it challenging to enhance the quality of the information environment as the information gap increases between them and influential CEOs.

Fourth, the sample is split into two subsamples using *SICREG* as the indicator variable equal to 1 if the banks operate as federally supervised banks or 0 if the banks only operate as state-supervised banks.

INSERT TABLE 10 ABOUT HERE

Panel A of Table 10 presents the results from the first stage of probit analysis with *SICREG* as the treatment effect and *CYBER_EVENT* as the independent variable. The results show that federally supervised banks are more likely to experience cyber events (*CYBER_EVENT: 0.202; p<0.1*). According to column 3 of Panel B Table 10, financial analysts face higher uncertainty for banks that operate as federally supervised banks (*SICREG: 0.224; p<0.01*). The dispersion among the financial analysts' forecasts is higher for these banks as the indirect cost of financial damage to these banks is unpredictable.

Next, the sample is split into two subsamples (well-capitalized banks vs. under-capitalized banks) using the *WELLCAP* as the indicator variable equal to 1 if the Tier 1 capital ratio of the bank is greater than 8% (well-capitalized) or 0 otherwise.

INSERT TABLE 11 ABOUT HERE

Panel A of Table 11 presents the results from the first stage of probit analysis with *WELLCAP* as the treatment effect and *CYBER_EVENT* as the independent variable. The results show that well-capitalized banks are more likely to attract cybercriminals (*CYBER_EVENT: 0.855; p<0.1*). According to column 3 of Panel B Table 11, financial analysts face less uncertainty for well-capitalized banks (*WELLCAP: -0.861; p<0.01*). Financial analysts also face less uncertainty about earnings forecasts for the banks with sufficient regulatory capital ratios as they believe they have sufficient capital reserves in the event of a crisis.

For the next analysis, the sample is split into two subsamples based on the number of analysts following using the *NUMANACAT* as an indicator variable equal to 1 if the number of analysts following the bank is above the overall sample average or 0 otherwise.

INSERT TABLE 12 ABOUT HERE

Panel A of Table 12 presents the results from the first stage of probit analysis with *NUMANACAT* as the treatment effect and *CYBER_EVENT* as the main independent variable. The results show that banks with more analysts following are less likely to suffer cyber attacks (*CYBER_EVENT: -0.436; p<0.1*). Attacked banks are more likely to have a low number of analysts following. Financial analysts are motivated to follow banks with a reputation and good profitability. These banks are also more likely to become a target for cybercriminals.

According to columns 3 and 4 of Panel B Table 12, the high number of analysts (*NUMANACAT*) decreases *INFORMATION ASYMMETRY* (-0.189; p < 0.01) but does not affect *UNCERTAINTY*. More financial analysts put effort into collecting bank risk management information and improving the quality of the overall information environment. The information gap decreases between financial analysts and top management of the banks.

Finally, our study also conducts separate analyses according to the type of cyber event, i.e., *CONFIDENTIALITY*, *AVAILABILITY*, or *INTEGRITY*. In this section, we look at how different types of cyber events affect individual financial analysts. First, we perform three first-stage PSM regressions for the three *CYBER EVENT TYPE*, i.e., *CONFIDENTIALITY, AVAILABILITY, and INTEGRITY.*

CYBER EVENT TYPE$_t$ = α_0 + FINANCIAL DAMAGE + BANK CHARACTERISTICS + FINANCIAL ANALYST CHARACTERTICS + ε (8)

Then, we use propensity score matching with the treatment effect *CYBER EVENT TYPE* and limit the sample to only banks that suffer cyber attacks to study how the likelihood of revision is related to different types of cyber attacks, earnings forecast dispersion, uncertainty, or asymmetry.

ANALYSTS EARNINGS PROPERTIES = α_0 + CYBER_EVENT TYPE + FINANCIAL DAMAGE + BANK CHARACTERISTICS + FINANCIAL ANALYST CHARACTERTICS + ε (7)

INSERT TABLE 13 ABOUT HERE

Panel B of Table 13 presents the results of the second stage analysis of the relationship between estimated confidentiality from the first stage ((*CONFIDENTIALITY* (1 vs. 0)) and analyst informational properties as proxied by *FERROR*, *DISPERSION*, *UNCERTAINTY*, and *INFORMATION ASYMMETRY*. *INFORMATION ASYMMETRY* is lower for *CONFIDENTIALITY* cyber events (-0.116, respectively; p < 0.01) than other types. Besides, *DISP* is also lower (-0.024; p < 0.01), indicating that financial analysts reach similar forecasts. Cyber attacks related to *CONFIDENTIALITY* result in lower information asymmetry, probably due to management efforts to provide more cybersecurity disclosure via conference calls or press releases. Financial analysts tend to improve their forecast quality for cyber attacks related to confidentiality as these cyber events often attract public attention.

Panel C of Table 13 presents the results of the second stage analysis of the relationship between estimated availability from the first stage ((*AVAILABILITY* (1 vs. 0)) and analyst informational properties as proxied by *FERROR*, *DISPERSION*, *UNCERTAINTY*, and *INFORMATION ASYMMETRY*. While *UNCERTAINTY* is higher for the AVAILABILITY cyber events (0.961; $p < 0.01$), the *INFORMATION ASYMMETRY* is lower (-0.122; $p < 0.01$) compared to other types. This result indicates that the *AVAILABILITY* cyber events are unpredictable for financial analysts. Overall, *DISP* is lower (-0.052; $p < 0.01$) as financial analysts reach similar forecasts using the same public cyber information provided by managers. *FERROR* is higher for *AVAILABILITY* cyber events (0.0064; $p < 0.01$), indicating the difficulty for financial analysts to estimate the impact of cyber breaches related to availability.

Panel D of Table 13 presents the results of the second stage analysis of the relationship between estimated integrity from the first stage ((*INTEGRITY* (1 vs. 0)) and analyst informational properties as proxied by *FERROR, DISP, UNCERTAINTY*, and *INFORMATION ASYMMETRY*. While uncertainty is lower for integrity cyber events (-0.607; $p < 0.01$), the *INFORMATION ASYMMETRY* is higher (0.155; $p < 0.01$) compared to other types. Meanwhile, *FERROR* is lower for integrity cyber events (-0.00093; $p < 0.01$). The outcome difference between *UNCERTAINTY* and *INFORMATION ASYMMETRY* could imply a higher quality of the information environment. Top management tends to protect their cybersecurity information against potential negative financial impacts, leading to higher information asymmetry. Cyber breaches associated with integrity issues can have a significant economic impact on a bank's reputation but rarely occur over time.

The results in Panel A of Table 13 show that financial analysts react more strongly toward cyber issues related to integrity and confidentiality despite the high information asymmetry between financial analysts and banks' management. However, they only successfully predict the change in reported earnings per share for integrity as it is much easier for them to quantify the direct costs of integrity through legal expenses and regulatory fines. Direct and indirect cyber losses related to availability remain a mystery among financial analysts.

4. Conclusion

Several factors such as the COVID-19 pandemic, advances in technology, and the advent of digital banking underlie an upward trend in cyber events among financial institutions, thus potentially undermining the trust between the banks and the public. While there is evidence that cyber events have capital market implications, this thesis investigates how cyber events play a role for financial analysts. As major information intermediaries, financial analysts are likely to play a major role in this regard. Hence, this thesis investigates how cyber events affect financial analysts' information environment in terms of uncertainty and asymmetry.

The thesis comprises two distinct yet related studies. The first study is an exploratory case study investigating financial analysts' approach to pressure top management regarding cybersecurity information during earnings conference calls. Financial analysts seamlessly connect top management and investors to share cybersecurity investing knowledge. In order to get top management at Bank of America and Bank of New York Mellon to open up more about their cybersecurity risk management and controls, financial analysts have started asking more questions about cyber-related topics like digital frauds or technical investments since 2014. Financial analysts were more concerned with the bank's defenses against possible cyberattacks than they were with directly evaluating the effectiveness of the bank's cyber security system.

From 2014 to 2022, JP Morgan's top management received the most inquiries from financial analysts about bank capital, mobile platforms, and capital budgeting from all five credit institutions in our analysis. Today's relatively high cyber susceptibility has financial analysts asking more concerns about data suppliers and cybersecurity. Financial analysts spent more time studying the cyber safety precautions at Bank of America and Bank of New York Mellon by asking top management more direct questions about their cybersecurity risk management due to JP

Morgan Chase cyber occurrences and New York State regulation. Since Citigroup was linked to the Equifax data breaches in 2017, there may have been greater pressure from financial analysts on the top management about cybersecurity issues. Following the Capital One cyber incident, the company's top management had a direct chat with a financial analyst in the third quarter of 2019 earnings conference call. This discussion resulted in more top management disclosure of cybersecurity and cloud technology.

Based on cyber events in the Advisen database, the second study indicates that financial analysts are more likely to revise their forecasts for banks that experience cyber attacks, and their earnings forecasts after the revisions have lower forecast errors than for financial analysts who do not revise their forecasts. Information asymmetry increases among financial analysts as the negative impacts of limited cyber information provided by top management outweigh the positive impacts of other factors affecting the banking industry (e.g., artificial intelligence and cloud technology). Despite facing high information asymmetry after security breaches, financial analysts work harder to gather information and revise earnings forecasts for affected banks, thus increasing the quality of the information environment and lowering uncertainty in their earnings forecasts. After cyber attacks, it appears that financial analysts neither feel obligated to revise their earnings forecast immediately nor wait patiently.

Despite the efforts of those financial analysts to revise their forecasts in response to cyber breaches, they did not necessarily perform better than those who decided not to revise. Financial analysts find it difficult to generate similar forecasts for banks that experience cyber attacks. Low information asymmetry minimizes the prediction risks and encourages financial analysts to revise their earnings forecasts more frequently. Financial analysts are hesitant to revise their earnings forecast when the information asymmetry is high due to limited private cyber data.

Because of the volatility of the cyber information environment after security breaches, financial analysts are less inclined to adjust their earnings forecasts for banks that encounter a confidentiality-related breach. Given their alleged insignificance, availability and integrity-related cyber incidents do not impact the likelihood of revision. Looking at how different cyber events affect individual financial analysts, we conclude that when banks suffer confidentiality-related cyber attacks like data breaches, the financial market exhibits less uncertainty and information asymmetry due to management's cybersecurity disclosure via conference calls or press releases. Otherwise, financial analysts and bank managers have more information asymmetry since top management protects cybersecurity information from financial risks. Integrity-related cyber issues often involve legal lawsuits, so they are under high public pressure, so financial analysts have more incentives to enhance the information environment. Finally, financial analysts find it difficult to make similar forecasts given the likelihood of unpredictable cybersecurity breaches linked to availability issues, resulting in high information asymmetry and forecast errors.

Our results are subject to limitations. We have limited observation for banks that undergo cyber attacks with accurate financial loss estimates, including timely legal or response costs. Furthermore, finding one-on-one matching based on all bank and analyst characteristics is difficult. Finally, there is a limited contribution to banking literature as cybersecurity is not often investigated for banks, even though banks are the most vulnerable to cyber attacks, as discussed in the exploratory case study.

Future research could look at textual analysts from all the banks to determine the value of cyber risk management in the current digital world. Future studies might also compare and expand on the role of cybersecurity in Asian or European banks. In cybersecurity, where oversight is looser, regulators should investigate the limited impact of Reg FD. In addition, future research could also examine the moderating role of environmental, social, and governance ratings that include cybersecurity dimensions on the relations uncovered in this thesis.

APPENDIX: VARIABLE DEFINITIONS FOR CYBERSECURITY EVENTS AND FINANCIAL ANALYSTS

Variable	Definition	Data source
AFFECTED_COUNT	Number of records exposed during the breach in quarter *t*	Advisen
ASSET INTANGIBILITY	One minus the amount of tangible assets scaled by quarter-end total assets (*ppentq*/*atq*)	Compustat
ASSET TANGIBILITY	The amount of tangible assets = Quarterly Gross property, plant, and equipment (ppentq) / total quarterly assets (*atq*)	Compustat
AVAILABILITY	Indicator variable coded one if the breach is related to "Network/Website Disruption" and "Cyber Extortion" and zero otherwise	Advisen
BTM	The ratio of quarterly book value (ceqq) to quarterly market value (*prccq x cshoq*)	Compustat
CAPR1Q	Quarterly risk-adjusted capital ratio Tier 1: core capital of the banks which represents financial institutions' ability to continue functioning in the event of an economic downturn (a minimum regulatory requirement under Basel III must be at least 6%)	Compustat
CAPR2Q	Quarterly risk-adjusted capital ratio Tier 2: an additional layer of the bank's capital which must be at least 2% so that the total regulatory capital be at least 8% under Basel III (total capital = Tier 1 Capital *CAPR1Q* + Tier 2 Capital *CAPR2Q*)	Compustat
CEOPOWER	The indicator variable is equal to one if the bank's CEO is also chair of the bank (CEO duality) and zero otherwise	BoardEx
CONFIDENTIALITY	The indicator variable coded one if the breach is related to "Data - Physical Lost or Stolen," "Data - Unintentional Disclosure," "Data - Malicious Breach," "Privacy - Unauthorized Contact or Disclosure," and "Privacy – Unauthorized Data Collection," and zero otherwise	Advisen
CYBER EVENT	Indicator variable equal to 1 if the firm experiences cybersecurity incidents	Advisen

	(cyberattacks) during quarter t, and zero otherwise.	
CYBGOV	Cyber Governance equal to 1 if the bank's top management team has a CIO, Chief Security Officer (CSO), Chief Security Information Officer (CSIO), Chief Privacy Officer (CPO), Chief Risk Officer (CRO), VP of Information, Director of IT, or IT Director in the fiscal year to which quarter *t* belongs, or 0 otherwise	BoardEx
DAMAGE	The dollar damage estimated for the attacked bank scaled by the bank's market value of equity	Advisen
DELAY OF REVISION	The number of days between the most recent forecast date and the last analyst earning forecast revision date during the quarter *t*	IBES
DISP	The standard deviation of analyst earning per share (*EPS*) forecasts scaled by the absolute value of mean *EPS* for the same quarter	IBES
EXPOSURE	Specific experience of financial analysts for a certain bank measured by the natural logarithm of one plus the number of quarters an analyst has covered the bank	IBES
FERROR	The absolute difference between the latest analysts' forecasts and the bank's actual earnings per share scaled by stock price	IBES
GENANA	General experience of financial analysts measured by the natural log of the number of quarters between the analyst j's first forecast in IBES and her current forecast at quarter *t*	IBES
INFORMATION ASYMMETRY	The individual analyst forecast dispersion around the average forecasts. The benchmark for information asymmetry is the absence of analyst consensus (Barron et al., 1998; Barron et al., 2009)	IBES
INTEGRITY	The indicator variable coded one if the breach is related to "Phishing, Spoofing, Social engineering," "Skimming, Physical Tampering," and "Identity - Fraudulent Use/Account Access," and zero otherwise	Advisen
LEV	Leverage equal to quarterly Short-term and long-term debt scaled by the market value of common equity: *(dlttq+dlcq)/ (dlttq+dlcq+ceqq)*	CRSP/Compustat

NCO	Quarterly net charge-off represents the difference between gross charge-offs (bad debt written off) and any subsequent recoveries of delinquent debt (*ncoq/lgq*)	Compustat
NIM	Net profit margin is quarterly net interest income (niintq) divided by the quarterly gross value of total loans (*lgq*)	Compustat
NPAT	Quarterly nonperforming total assets, which represent loans or advances that are in default or arrears and the current financial fitness of the bank (*npatq/lgq*)	Compustat
NUMANA	Natural log of the total number of analysts following the banks during the quarter *t*	IBES
NUMANACAT	Analyst Following Category equal to 1 if the number of analysts following the bank is above the overall sample average or zero otherwise	IBES
PLL	Quarterly loan loss provisions scaled by total loans (pllq/lgq)	Compustat
REVISE	Revision Likelihood equal to 1 if the analyst revises their analyst forecast during quarter *t*, and zero otherwise	IBES
SICREG	Bank Supervision equal to 1 if the bank is federally supervised bank or zero if it is state supervised	Compustat
SIZE	The natural logarithm of total assets (*at*)	Compustat
SIZECAT	Bank Size Category equal to 1 if the size of the bank is above the overall sample average or zero otherwise	Compustat
STOCK_TURNOVER	Number of shares traded in quarter *t* divided by the bank's average number of shares outstanding in quarter *t*	CRSP
UNCERTAINTY	Common uncertainty or idiosyncratic risks (errors in the mean forecast) measured as the average of the variances between individual analyst estimates and actual earnings per share (Barron *et al.*, 2009)	IBES
WELLCAP	Bank Capitalization equal to 1 if the Tier 1 capital ratio of the bank is greater than 8% (well-capitalized) or zero otherwise.	Compustat

TABLES

TABLE 1

Sample Development

Panel A: Sample Development		
Number of individual analyst forecasts for banks at IBES from 2007 to 2022	368,724	
Less: Number of individual analysts forecast duplications	(284,009)	
Number of available individual analyst forecasts		84,715
Number of financial data on banks at Compustat	42,047	
Less: Number of bank observations with missing financial data and duplications	(4,736)	
Number of available individual analyst observations with financial data		37,311
Number of observations with stock data for banks at CRSP from 2007 to 2022	91,825	
Less: Number of observations with missing stock data and duplications	(61,152)	
Number of available individual stock data		30,673
Number of board data for banks at BoardEx from 2007 to 2022	823,736	
Less: Number of missing board data and duplications	(524,087)	
Number of available board data		299,649
Number of cyber events for banks available at Advisen		1,110
Number of data available for analysts and banks data merged among IBES, Advisen, Compustat, and CRSP	78,300	
Less: Number of missing data for earnings forecast error and earnings forecast dispersion	(1,550)	
Final sample for all individual analyst earnings forecast data		76,750
Panel B: Other sample sets		
Number of data available for analysts and banks data merged among IBES, Advisen, and Compustat	78,300	
Less: Number of data available for individual analysts who do not make earnings forecast revision	(52,238)	
Final sample for individual analysts who make earnings forecast revision (*Revise*=1)		26,062
Number of data available for analysts and banks data merged among IBES, Advisen, and Compustat	78,300	
Less: Number of data available for individual analysts who are not involved with security breaches	(72,117)	
Final sample for individual analysts who are involved with security breaches (*Cyber_Event*=1)		6,183

Table 2

Summary Statistics

Panel A: All individual analyst earnings forecast data

	(1)	**(2)**	**(3)**	**(4)**	**(5)**
Variable	**Obs**	**Mean**	**Std. Dev.**	**Min**	**Max**
CYBER EVENT	76750	0.081	0.272	0	1
REVISE	76750	0.339	0.474	0	1
DISP	76750	0.174	0.422	0	4.669
FERROR	76750	0.005	0.012	0	0.169
SIZE	76750	9.841	1.837	5.665	15.19
BTM	76750	0.903	0.456	-2.26	11.133
LEV	76750	0.457	0.186	0	1.095
NIM	76750	0.012	0.005	-0	0.19
ASSET TANGIBILITY	76750	0.012	0.007	0	0.09
CAPR1Q	76750	12.287	2.746	2.73	55.35
CAPR2Q	76750	2.3	1.994	-2.03	29.04
NPAT	76750	0.016	0.018	0	0.482
PLL	76750	0.001	0.003	-0.01	0.045
NCO	76750	-0.001	0.002	-0.06	0.018
STOCK TURNOVER	76750	12.639	2.157	6.17	19.516
NUMANA	76750	2.159	0.743	0.693	3.466
EXPOSURE	76750	25.064	15.886	1	62
GENANA	76750	2.898	0.953	0	4.111
UNCERTAINTY	76750	0.706	7.515	0	442.569
INFORMATION ASYMMETRY	76750	0.697	0.447	0	2
SIZECAT	76750	0.67	0.47	0	1
CYBGOV	76347	0.529	0.499	0	1
CEOPOWER	76347	0.532	0.499	0	1
SICREG	76750	0.977	0.151	0	1
WELLCAP	76750	0.973	0.162	0	1
NUMANACAT	76750	0.518	0.5	0	1

Panel B: Individual analysts who revise their forecast (Revise=1)

	(1)	**(2)**	**(3)**	**(4)**	**(5)**
Variable	**Obs**	**Mean**	**Std. Dev.**	**Min**	**Max**
CYBER EVENT	26062	0.133	0.339	0	1
DELAY OF REVISION	26062	52.174	25.122	0	218
SIZE	26062	10.548	1.978	6.066	15.19
BTM	26062	0.945	0.506	0.188	11.133
LEV	26062	0.48	0.185	0	0.902
NIM	26062	0.012	0.005	-0	0.19
ASSET TANGIBILITY	26062	0.011	0.007	0	0.09
CAPR1Q	26062	12.032	2.622	4.3	55.35
CAPR2Q	26062	2.309	1.598	-2.03	26.35
NPAT	26062	0.014	0.016	0	0.482

PLL	26062	0.002	0.003	-0.01	0.045
NCO	26062	-0.001	0.002	-0.06	0.007
STOCK TURNOVER	26062	13.332	2.146	6.17	19.516
NUMANA	26062	2.409	0.693	0.693	3.466
EXPOSURE	26062	28.658	16.694	1	62
GENANA	26062	2.972	0.932	0	4.111
UNCERTAINTY	26062	1.401	11.545	0	442.569
INFORMATION ASYMMETRY	26062	0.595	0.422	0	2
Panel C: Individual analysts who issue forecasts for banks who suffer cyberattacks (Cyber_Event=1)					
	(1)	**(2)**	**(3)**	**(4)**	**(5)**
Variable	**Obs**	**Mean**	**Std. Dev.**	**Min**	**Max**
REVISE	6183	0.559	0.497	0	1
SIZE	6183	12.992	1.634	6.998	15.136
BTM	6183	0.948	0.377	0.267	3.398
LEV	6183	0.578	0.147	0.034	0.825
NIM	6183	0.013	0.008	0.007	0.097
ASSET TANGIBILITY	6183	0.009	0.005	0.001	0.042
CAPR1Q	6183	12.028	1.823	6.87	20.5
CAPR2Q	6183	2.631	0.981	0.3	12.53
NPAT	6183	0.013	0.01	0	0.102
PLL	6183	0.002	0.002	-0	0.025
NCO	6183	-0.002	0.002	-0.03	0.001
DAMAGE	6183	15.266	181.33	0	4790.39
AFFECTED COUNT	6183	11830.98	110656	0	1500000
CONFIDENTIALITY	6183	0.765	0.424	0	1
AVAILABILITY	6183	0.046	0.21	0	1
INTEGRITY	6183	0.088	0.283	0	1
UNCERTAINTY	6183	0.744	3.164	0.004	38.737
INFORMATION ASYMMETRY	6183	0.517	0.361	0.006	1.964

Table 3

Correlation

Panel A: All individual analyst earnings forecast data

Correlation

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)	(26)
(1) CYBER_EVENT	1																									
(2) REVISE	0.137	1																								
(3) DISP	-0.021	0.081	1																							
(4) FERROR	-0.045	0.051	0.327	1																						
(5) SIZE	0.508	0.276	-0.011	-0.067	1																					
(6) BTM	0.029	0.066	0.3	0.483	0.014	1																				
(7) LEV	0.193	0.088	0.117	0.127	0.3	0.12	1																			
(8) NIM	0.07	-0.013	-0.039	-0.069	-0.001	-0.143	-0.103	1																		
(9) ASSET_TANGIBILITY	-0.124	-0.093	0.057	0.06	-0.292	0.112	-0.147	0.062	1																	
(10) CAPR1Q	-0.028	-0.066	0.002	-0.058	-0.169	-0.07	-0.327	0.385	0.097	1																
(11) CAPR2Q	0.049	0.003	0.066	0.052	0.109	0.138	0.232	-0.101	-0.108	-0.241	1															
(12) NPAT	-0.044	-0.062	0.288	0.294	-0.138	0.365	0.101	0.044	0.183	0.186	0.111	1														
(13) PLL	0.013	0.091	0.371	0.473	0.047	0.368	0.242	0.014	0.049	-0.067	0.087	0.467	1													
(14) NCO	-0.059	-0.049	-0.311	-0.374	-0.101	-0.332	-0.215	-0.04	-0.051	-0.028	-0.108	-0.544	-0.81	1												
(15) STOCK_TURNOVER	0.416	0.231	0.056	-0.015	0.904	0.099	0.316	-0.005	-0.272	-0.164	0.177	-0.046	0.15	-0.2	1											
(16) NUMANA	0.34	0.241	0.025	-0.053	0.817	0.007	0.232	0.013	-0.256	-0.162	0.058	-0.038	0.093	-0.151	0.818	1										
(17) EXPOSURE	0.176	0.162	-0.039	-0.08	0.394	-0.088	0.038	0.054	-0.118	0.002	-0.064	-0.073	-0.032	-0.002	0.326	0.37	1									
(18) GENANA	0.039	0.055	-0.11	-0.105	0.11	-0.064	-0.311	-0.096	-0.062	0.13	-0.1	-0.205	-0.246	0.22	0.017	0.015	0.323	1								
(19) UNCERTAINTY	0.002	0.066	0.056	0.159	0.073	-0.003	-0.024	0.001	-0.019	0.005	-0.017	0.01	0.053	-0.038	0.024	0.063	0.025	0.024	1							
(20) INFORMATION_ASYMMETRY	-0.119	-0.164	-0.08	-0.291	-0.339	-0.086	-0.078	0.013	0.092	0.078	-0.018	-0.023	-0.154	0.155	-0.288	-0.394	-0.153	-0.029	-0.13	1						
(21) SIZECAT	0.201	0.183	-0.009	-0.062	0.701	-0.01	0.191	-0.007	-0.221	-0.173	0.099	-0.071	0.05	-0.077	0.732	0.725	0.301	0.028	0.053	-0.274	1					
(22) CYBGOV	0.209	0.126	0.008	-0.044	0.455	-0.005	0.099	0.014	-0.121	-0.044	0.037	-0.09	-0.022	-0.027	0.419	0.392	0.224	0.111	0.039	-0.17	0.313	1				
(23) CEOPOWER	0.083	0.079	-0.005	0.008	0.262	-0.019	0.144	-0.02	-0.062	-0.102	0.088	-0.044	0.02	-0.011	0.248	0.27	0.118	-0.036	-0.015	-0.082	0.186	0.137	1			
(24) SICREG	0.037	0.035	0.03	0.023	0.044	-0.011	-0.106	0.07	0.039	0.112	-0.167	0.029	0.052	-0.06	-0.005	0.053	0.069	0.007	0.013	-0.049	0.025	-0.011	0.015	1		
(25) WELLCAP	0.028	-0.044	-0.04	-0.057	-0.074	-0.054	-0.216	0.072	0.026	0.294	-0.201	0.002	-0.094	0.026	-0.097	-0.059	0.062	0.21	-0.012	0.033	-0.064	-0.009	-0.039	0.071	1	
(26) NUMANACAT	0.26	0.223	0.029	-0.026	0.715	0.023	0.231	0	-0.246	-0.19	0.07	-0.064	0.092	-0.121	0.715	0.85	0.321	-0.005	0.063	-0.336	0.687	0.334	0.245	0.026	-0.078	1

Panel B: Individual analysts who revise their forecast (Revise=1)

Correlation

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)
(1) CYBER_EVENT	1																	
(2) DELAY_OF_REVISION	*0.049*	1																
(3) SIZE	*0.546*	*0.116*	1															
(4) BTM	*0.024*	*-0.046*	0.003	1														
(5) LEV	*0.255*	*0.024*	*0.366*	*0.133*	1													
(6) NIM	*0.113*	-0.009	*0.052*	*-0.138*	*-0.01*	1												
(7) ASSET_TANGIBILITY	*-0.155*	*-0.051*	*-0.331*	*0.12*	*-0.171*	*0.027*	1											
(8) CAPR1Q	*0.023*	*-0.029*	*-0.076*	*-0.107*	*-0.281*	*0.395*	*0.029*	1										
(9) CAPR2Q	*0.073*	0.004	*0.122*	*0.169*	*0.27*	*-0.07*	*-0.061*	*-0.298*	1									
(10) NPAT	*-0.036*	*-0.036*	*-0.131*	*0.343*	*0.137*	0.004	*0.16*	*0.1*	*0.19*	1								
(11) PLL	-0.008	*-0.054*	-0.005	*0.383*	*0.268*	-0.001	*0.06*	*-0.105*	*0.155*	*0.479*	1							
(12) NCO	*-0.059*	*0.02*	*-0.075*	*-0.318*	*-0.26*	*-0.033*	*-0.035*	0.007	*-0.172*	*-0.553*	*-0.809*	1						
(13) STOCK_TURNOVER	*0.465*	*0.095*	*0.902*	*0.135*	*0.402*	*0.047*	*-0.284*	*-0.101*	*0.209*	-0.004	*0.135*	*-0.203*	1					
(14) NUMANA	*0.356*	*0.132*	*0.8*	-0.006	*0.286*	*0.021*	*-0.305*	-0.101	*0.088*	-0.026	*0.028*	*-0.118*	*0.808*	1				
(15) EXPOSURE	*0.206*	*0.07*	*0.427*	*-0.1*	*0.09*	*0.054*	*-0.17*	*0.034*	*-0.059*	*-0.086*	*-0.063*	0.008	*0.365*	*0.409*	1			
(16) GENANA	*0.052*	*0.038*	*0.134*	-0.093	-0.334	-0.111	*-0.056*	*0.155*	-0.178	-0.285	-0.295	*0.278*	0.008	*0.035*	*0.324*	1		
(17) UNCERTAINTY	*-0.011*	-0.009	*0.057*	*-0.018*	*-0.05*	0.004	0.003	*0.025*	*-0.036*	*0.023*	*0.036*	*-0.026*	-0.004	*0.049*	0.01	*0.033*	1	
(18) INFORMATION ASYMMETRY	*-0.112*	*-0.057*	*-0.324*	*-0.058*	*-0.072*	*0.018*	*0.122*	*0.046*	*-0.035*	-0.006	*-0.109*	*0.122*	*-0.27*	*-0.37*	*-0.165*	*-0.049*	*-0.153*	1

Panel C: Individual analysts who issue forecasts for banks who suffer cyberattacks (Cyber_Event=1)

Correlation

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)
(1) REVISE	1																	
(2) SIZE	*0.221*	1																
(3) BTM	*0.084*	*0.116*	1															
(4) LEV	*0.168*	*0.653*	*0.039*	1														
(5) NIM	*0.045*	*0.035*	*-0.123*	*0.260*	1													
(6) ASSET_TANGIBILITY	*-0.134*	*-0.446*	*-0.061*	*-0.327*	*0.047*	1												
(7) CAPR1Q	*0.098*	*0.266*	0.014	*0.115*	*0.577*	*-0.084*	1											
(8) CAPR2Q	*-0.028*	*0.103*	*0.284*	*0.233*	*-0.155*	*0.140*	*-0.337*	1										
(9) NPAT	*-0.040*	*0.086*	*0.333*	*0.159*	*-0.075*	*0.060*	*-0.139*	*0.539*	1									
(10) PLL	*0.072*	*0.191*	*0.222*	*0.387*	*0.095*	*-0.021*	*-0.174*	*0.321*	*0.429*	1								
(11) NCO	*-0.046*	*-0.253*	*-0.295*	*-0.426*	*-0.075*	*0.027*	*0.136*	*-0.465*	*-0.660*	*-0.763*	1							
(12) DAMAGE	*-0.058*	*-0.097*	*-0.030*	*-0.037*	-0.005	0.001	-0.017	*-0.023*	*0.062*	0.005	-0.005	1						
(13) AFFECTED_COUNT	0.021	-0.011	*-0.060*	*-0.061*	*-0.023*	*-0.035*	*-0.032*	*-0.080*	*-0.057*	*-0.048*	*0.045*	-0.009	1					
(14) CONFIDENTIALITY	0.014	0.02	*0.030*	*0.044*	*0.075*	0.009	*0.161*	*-0.111*	*-0.134*	0.005	*0.021*	*-0.065*	*-0.150*	1				
(15) AVAILABILITY	-0.023	*-0.067*	*-0.028*	*-0.117*	*-0.035*	*0.130*	*-0.042*	0.008	*0.068*	*-0.040*	0.006	-0.019	-0.006	*-0.398*	1			
(16) INTEGRITY	*-0.027*	*0.028*	*0.028*	0.004	*-0.046*	*-0.027*	*-0.064*	*0.118*	*0.186*	0.004	*-0.080*	*0.087*	*-0.032*	*-0.561*	*-0.068*	1		
(17) UNCERTAINTY	*0.117*	*0.155*	*-0.040*	*0.133*	-0.007	*-0.042*	*0.118*	*-0.023*	-0.009	0.005	*-0.029*	-0.019	-0.005	*0.035*	-0.019	*-0.064*	1	
(18) INFORMATION ASYMMETRY	*-0.131*	*-0.221*	*-0.049*	*-0.152*	*0.049*	*0.141*	*-0.041*	0.011	0.02	*-0.049*	*0.083*	*0.089*	*-0.088*	*-0.112*	*0.089*	*0.144*	*-0.270*	1

Italic indicates statistical significance at the 10 percent, 5 percent, or 1 percent levels in a two-tailed test.

Table 4

The Relation between Cyber Events and Individual Analyst Earnings Forecast Properties

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)

	(1)				
Variable	***CYBER EVENT***				
SIZE	0.572***				
	(42.22)				
BTM	0.079***				
	(3.25)				
LEV	0.029				
	(0.39)				
NIM	-9.672**				
	(-2.37)				
ASSET TANGIBILITY	14.1***				
	(8.75)				
CAPR1Q	-0.035***				
	(-4.86)				
CAPR2Q	0.01				
	(1.36)				
NPAT	7.636*				
	(1.67)				
PLL	-57.373***				
	(-8.85)				
NCO	-2.425				
	(-0.26)				
NIM X CAPR1Q	1.411***				
	(6.23)				
SIZE X NPAT	-0.632				
	(-1.48)				
STOCK_TURNOVER	-0.006				
	(-0.51)				
NUMANA	0.171***				
	(6.17)				
EXPOSURE	-0.0003				
	(-0.53)				
GENANA	0.017				
	(1.46)				
INTERCEPT	-8.045***				
	(-55.72)				
Pseudo R2	0.4283				

Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)

	(1)	**(2)**	**(3)**	**(4)**	**(5)**
Variable	***FERROR***	***DISP***	***REVISE***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***

CYBER EVENT (1 VS 0)	0.0003	-0.018***	0.071***	-0.356***	0.038***
	(0.76)	(-4.13)	(2.12)	(-9.75)	(2.97)
SIZE	0.0017***	0.012**	0.297***	1.829***	-0.171***
	(14.59)	(2.22)	(12.87)	(14.47)	(-29.07)
BTM	0.0092***	0.17***	0.364***	0.304	-0.145***
	(47.29)	(19.73)	(9.61)	(1.47)	(-15.01)
LEV	0.0043***	0.088***	0.015	-8.302***	0.103***
	(5.96)	(2.76)	(0.11)	(-10.89)	(2.9)
NIM	-0.111**	-6.49***	6.796	54.94	8.967***
	(-2.5)	(-3.3)	(0.84)	(1.62)	(4.08)
ASSET TANGIBILITY	0.112***	1.71***	-6.491**	-25.867	-1.155
	(7.56)	(2.61)	(-2.27)	(-1.65)	(-1.57)
CAPR1Q	-0.0004***	0.0002	-0.0007	0.205***	0.0156**
	(-5.46)	(0.57)	(-0.05)	(2.87)	(4.67)
CAPR2Q	0.0003***	0.006	-0.016	0.15	-0.006
	(3.05)	(1.44)	(-0.94)	(1.62)	(-1.57)
NPAT	0.524***	-0.92	16.733**	-1.549	-25.175***
	(12.56)	(-0.5)	(2.08)	(-0.04)	(-12.2)
PLL	0.462***	70.041***	44.933**	70.799	6.285***
	(9.36)	(32.09)	(4.45)	(1.35)	(2.58)
NCO	-0.249***	14.631***	-14.329	-453.618***	56.345***
	(-3.46)	(4.6)	(-1.00)	(-5.96)	(15.87)
NIM X CAPR1Q	0.008***	0.298***	0.021	-2.614	-0.5***
	(3.25)	(2.75)	(0.05)	(-1.01)	(-4.13)
SIZE X NPAT	-0.044***	0.165	-2.441***	-2.701	2.43***
	(-12.6)	(1.06)	(-3.6)	(-0.73)	(13.99)
STOCK_TURNOVER	-0.0014***	-0.007	-0.165***	-1.621***	0.134***
	(-13.85)	(-1.5)	(-8.49)	(-15.18)	(26.83)
NUMANA	-0.0022***	-0.06***	-0.023	0.016	-0.14***
	(-8.55)	(-5.1)	(-0.48)	(0.06)	(-11.26)
EXPOSURE	0.000007	0.00054***	0.01***	0.0024	-0.00015
	(1.49)	(2.67)	(11.27)	(0.5)	(-0.66)
GENANA	0.0001	0.015***	0.064***	-0.117	-0.01***
	(1.02)	(3.55)	(3.49)	(-1.15)	(-2.15)
INTERCEPT	0.0006	-0.08	-1.837***	4.85***	0.942***
	(0.48)	(-1.51)	(-7.86)	(3.77)	(15.72)
Adjusted R2	0.3004	0.2839	0.0710	0.0533	0.1561

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 5

The Relation between Cyber Events and Individual Analyst Earnings Forecast Properties after Revision

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)

	(1)				
Variable	***CYBER EVENT***				
SIZE	0.555***				
	(28.35)				
BTM	0.093***				
	(2.78)				
LEV	0.023				
	(0.2)				
NIM	4.999				
	(0.93)				
ASSET TANGIBILITY	11.111***				
	(4.47)				
CAPR1Q	-0.0193*				
	(-1.85)				
CAPR2Q	0.042***				
	(3.59)				
NPAT	14.426**				
	(2.66)				
PLL	-53.284***				
	(-6.43)				
NCO	-12.282				
	(-0.96)				
NIM X CAPR1Q	0.797***				
	(2.67)				
SIZE X NPAT	-1.2**				
	(-2.25)				
STOCK_TURNOVER	-0.004				
	(-0.22)				
NUMANA	0.25***				
	(5.66)				
EXPOSURE	0.0006				
	(0.69)				
GENANA	0.025				
	(1.33)				
INTERCEPT	-8.52***				
	(-40.85)				
Pseudo R2	0.4066				
Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)					
	(1)	**(2)**	**(3)**	**(4)**	**(5)**
Variable	***FERROR***	***DISP***	***DELAY OF REVISION***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***

CYBER EVENT (1 VS 0)	-0.0013***	-0.035	2.572	-0.928***	0.034
	(-3.19)	(-1.26)	(1.37)	(-4.47)	(1.51)
SIZE	0.001***	0.008*\	1.177*	4.96***	-0.18***
	(6.89)	(1.00)	(1.9)	(16.06)	(-21.98)
BTM	0.0058***	0.168***	-4.718***	1.564***	-0.111***
	(23.24)	(13.28)	(-4.64)	(3.08)	(-8.28)
LEV	0.002**	0.111	-8.343**	-11.498***	0.092*
	(2.08)	(2.27)	(-2.12)	(-5.85)	(1.78)
NIM	-0.123***	-8.153***	387.694**	-161.163*	11.783***
	(-2.91)	(-3.8)	(2.25)	(-1.87)	(5.18)
ASSET TANGIBILITY	0.116***	2.849***	-127.95*	839.045***	-2.946***
	(6.54)	(3.19)	(-1.78)	(23.41)	(-3.11)
CAPR1Q	-0.00024**	-0.01**	0.844**	0.221	0.026***
	(-2.88)	(-2.5)	(2.53)	(1.32)	(5.92)
CAPR2Q	0.0004***	0.005	1.034**	-0.132	0.005
	(3.46)	(0.92)	(2.41)	(-0.62)	(0.92)
NPAT	0.437***	-1.659	159.006	-486.328***	-27.569***
	(6.83)	(-0.51)	(0.61)	(-3.76)	(-8.06)
PLL	0.557***	75.055***	-227.303	441.006***	12.135***
	(10.55)	(28.19)	(-1.06)	(4.13)	(4.3)
NCO	-0.124	24.11***	-662.247**	-251.663	61.532***
	(-1.49)	(5.76)	(-1.97)	(-1.5)	(13.87)
NIM X CAPR1Q	0.008***	0.458***	-26.298***	7.196	-0.741***
	(3.32)	(3.88)	(-2.77)	(1.52)	(-5.91)
SIZE X NPAT	-0.035	0.329	-16.349	39.898***	2.546***
	(-6.86)	(1.27)	(-0.79)	(3.85)	(9.28)
STOCK_TURNOVER	-0.0005***	0.003	-0.944*	-3.881***	0.132***
	(-4.13)	(0.44)	(-1.77)	(-14.61)	(18.74)
NUMANA	-0.003***	-0.084***	1.97	-5.476***	-0.075***
	(-8.93)	(-4.89)	(1.43)	(-7.96)	(-4.13)
EXPOSURE	0.000007	-0.0003	-0.045*	-0.021*	-0.0002
	(1.2)	(-1.09)	(-1.93)	(-1.77)	(-0.56)
GENANA	0.0005***	0.034***	1.852***	-0.155	-0.009
	(3.96)	(5.13)	(3.46)	(-0.58)	(-1.33)
INTERCEPT	-0.00007	0.0005	41.95***	10.991***	0.706***
	(-0.04)	(0.01)	(6.58)	(3.46)	(8.39)
Adjusted R2	0.2406	0.3291	0.0178	0.1542	0.1346

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 6

The Relation between Revision Likelihood and Individual Analyst Earnings Forecast Properties for banks that Suffer Security Breaches

Panel A: First Stage of Propensity Score Matching (PSM) Analysis				
	(1)			
Variable	***REVISE***			
SIZE	0.32***			
	(11.07)			
BTM	0.646***			
	(10.72)			
LEV	0.405**			
	(2.13)			
NIM	5.814**			
	(1.91)			
ASSET_TANGIBILITY	2.457			
	(0.65)			
CAPR1Q	-0.005			
	(-0.37)			
CAPR2Q	-0.019			
	(-0.83)			
NPAT	-11.42***			
	(-4.54)			
PLL	47.376***			
	(3.81)			
NCO	-2.56			
	(-0.15)			
CONFIDENTIALITY	-0.133**			
	(-2.3)			
AVAILABILITY	-0.037			
	(-0.38)			
INTEGRITY	-0.035			
	(-0.45)			
DAMAGE	-0.00049***			
	(-2.23)			
AFFECTED_COUNT	0.0000001			
	(1.09)			
STOCK_TURNOVER	-0.243***			
	(-9.25)			
NUMANA	-0.085			
	(-1.34)			
EXPOSURE	0.0126***			
	(11.16)			
GENANA	0.022			
	(0.89)			
INTERCEPT	-1.118***			

	(-4.87)			
Pseudo R2	0.0804			
Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation) with Revise as treatment				
	(1)	**(2)**	**(3)**	**(4)**
Variable	***FERROR***	***DISP***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
REVISE (1 VS 0)	0.0004	0.036***	0.453***	-0.025**
	(1.31)	(3.77)	(5.17)	(-2.43)
SIZE	0.00117***	0.027***	1.093***	-0.145***
	(9.09)	(4.13)	(12.73)	(-17.18)
BTM	0.0065***	0.241***	0.417***	-0.16***
	(27.05)	(19.4)	(2.59)	(-10.10)
LEV	0.0069***	0.225***	2.629***	-0.146***
	(7.9)	(5.03)	(4.53)	(-2.58)
NIM	-0.0009	-0.689	-52.345***	2.388***
	(-0.07)	(-1.05)	(-6.12)	(2.85)
ASSET_TANGIBILITY	0.166***	4.998***	76.702***	-4.861***
	(9.88)	(5.78)	(6.83)	(-4.42)
CAPR1Q	-0.000126**	0.0004	0.301***	-0.00007
	(-2.07)	(0.13)	(7.39)	(-0.02)
CAPR2Q	0.0003***	0.013**	0.027	-0.0054
	(2.75)	(2.47)	(0.4)	(-0.81)
NPAT	0.02**	-0.529	1.545	3.757***
	(1.96)	(-0.9)	(0.2)	(5.04)
PLL	0.598***	71.195***	-43.96	4.113
	(13.33)	(30.84)	(-1.47)	(1.4)
NCO	0.242***	19.358***	-209.316***	41.046***
	(3.66)	(5.7)	(-4.75)	(9.5)
CONFIDENTIALITY	0.0002	-0.042***	-0.571***	-0.027*
	(1.01)	(-3.37)	(-3.54)	(-1.69)
AVAILABILITY	0.0008*	-0.017	-0.453	0.157***
	(1.91)	(-0.79)	(-1.64)	(5.79)
INTEGRITY	-0.0006*	-0.02	-1.044***	0.137***
	(-1.78)	(-1.17)	(-4.75)	(6.37)
DAMAGE	0.000001	-0.00003	0.0006	0.004***
	(1.22)	(-0.52)	(0.75)	(5.36)
AFFECTED_COUNT	0.000000001***	0.00000001	-0.00000001	-0.0000003***
	(3.67)	(0.35)	(-0.36)	(-7.99)
STOCK_TURNOVER	-0.0012***	-0.023***	-1.024***	0.154***
	(-10.74)	(-3.98)	(-13.51)	(20.7)
NUMANA	-0.0032***	-0.076***	-0.966***	-0.124***
	(-11.43)	(-5.21)	(-5.1)	(-6.66)
EXPOSURE	-0.000002	0.00004	-0.001	-0.0000002
	(-0.38)	(0.17)	(-0.46)	(-0.00)

GENANA	0.0003***	0.0196***	0.13*	-0.005
	(3.13)	(3.45)	(1.77)	(-0.71)
INTERCEPT	0.004***	-0.168***	-0.51	0.663***
	(3.5)	(-3.23)	(-0.76)	(10.05)
Adjusted R2	0.2712	0.3705	0.1103	0.1888

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 7

The Relation between Bank Size Category and Individual Analyst Earnings Forecast Properties

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)

	(1)			
Variable	***SIZECAT***			
CYBER_EVENT	0.706***			
	(5.24)			
BTM	-0.146***			
	(-5.64)			
LEV	0.399***			
	(6.89)			
NIM	-6.08**			
	(-2.32)			
ASSET TANGIBILITY	17.343***			
	(14.16)			
CAPR1Q	-0.049***			
	(-13.69)			
CAPR2Q	-0.049***			
	(-13.69)			
NPAT	0.025***			
	(4.72)			
PLL	-65.643***			
	(-10.79)			
NCO	-35.285***			
	(-4.92)			
STOCK_TURNOVER	1.238***			
	(98.73)			
NUMANA	1.038***			
	(46.36)			
EXPOSURE	0.013***			
	(17.75)			
GENANA	0.021*			
	(1.95)			
INTERCEPT	-16.154***			
	(-103.77)			
Pseudo R2	0.6414			

Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)

	(1)	**(2)**	**(3)**	**(4)**
Variable	***REVISE***	***FERROR***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
SIZECAT (1 VS 0)	0.031*	-0.0014***	0.939***	-0.053***
	(1.83)	(-5.04)	(6.92)	(-3.95)

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 8

The Relation between Cyber Governance and Individual Analyst Earnings Forecast Properties

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)

	(1)			
Variable	***CYBGOV***			
CYBER_EVENT	-0.027			
	(-0.98)			
SIZE	0.304***			
	(31.81)			
BTM	0.044***			
	(3.44)			
LEV	0.033			
	(1.04)			
NIM	2.376*			
	(1.75)			
ASSET TANGIBILITY	3.947***			
	(5.57)			
CAPR1Q	0.018***			
	(8.02)			
CAPR2Q	0.003			
	(1.26)			
NPAT	-2.615***			
	(-6.88)			
PLL	-43.416***			
	(-12.3)			
NCO	-39.159***			
	(-9.28)			
STOCK_TURNOVER	0.035***			
	(5.63)			
NUMANA	0.06***			
	(4.39)			
EXPOSURE	0.003***			
	(7.8)			
GENANA	0.075***			
	(11.98)			
INTERCEPT	-4.051***			
	(-62.93)			
Pseudo R2	0.1259			

Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)

	(1)	**(2)**	**(3)**	**(4)**
Variable	***REVISE***	***FERROR***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
CYBGOV (1 VS 0)	-0.001	-0.0002	0.224***	-0.021***
	(-0.26)	(-1.47)	(4.74)	(-4.94)

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 9

The Relation between CEO Power and Individual Analyst Earnings Forecast Properties

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)				
	(1)			
Variable	***CEOPOWER***			
CYBER_EVENT	-0.272***			
	(-13.07)			
SIZE	0.131***			
	(17.55)			
BTM	-0.085***			
	(-7.12)			
LEV	0.42***			
	(13.92)			
NIM	-3.966***			
	(-3.55)			
ASSET TANGIBILITY	6.997***			
	(10.37)			
CAPR1Q	-0.003			
	(-1.29)			
CAPR2Q	0.045***			
	(16.98)			
NPAT	-1.26***			
	(-3.59)			
PLL	24.957***			
	(7.86)			
NCO	43.685***			
	(11.2)			
STOCK_TURNOVER	-0.035***			
	(-6.06)			
NUMANA	0.31***			
	(25.53)			
EXPOSURE	0.003***			
	(7.81)			
GENANA	-0.069***			
	(-11.7)			
INTERCEPT	-1.455***			
	(-27.89)			
Pseudo R2	0.0715			
Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)				
	(1)	**(2)**	**(3)**	**(4)**
Variable	***REVISE***	***FERROR***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
CEOPOWER (1 VS 0)	-0.002	0.0005***	-0.633***	0.025***
	(-0.4)	(5.89)	(-7.99)	(6.83)

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 10

The Relation between Bank Supervision and Individual Analyst Earnings Forecast Properties

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)

	(1)			
Variable	***SICREG***			
CYBER_EVENT	0.202**			
	(1.97)			
SIZE	0.706***			
	(23.39)			
BTM	-0.073**			
	(-2.27)			
LEV	-1.742***			
	(-18.81)			
NIM	18.491***			
	(3.35)			
ASSET TANGIBILITY	-2.594			
	(-1.28)			
CAPR1Q	0.141***			
	(21.18)			
CAPR2Q	-0.054***			
	(-13.98)			
NPAT	-2.253**			
	(-2.29)			
PLL	161.117***			
	(12.31)			
NCO	-177.278			
	(-10.02)			
STOCK_TURNOVER	-0.507***			
	(-27.65)			
NUMANA	0.22***			
	(6.67)			
EXPOSURE	0.011***			
	(10.15)			
GENANA	-0.236***			
	(-15.24)			
INTERCEPT	0.781***			
	(4.04)			
Pseudo R2	0.2780			

Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)

	(1)	**(2)**	**(3)**	**(4)**
Variable	***REVISE***	***FERROR***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
SICREG (1 VS 0)	0.092***	-0.002	0.224***	-0.039
	(3.89)	(-1.14)	(22.72)	(-0.91)

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 11

The Relation between Bank Capitalization and Individual Analyst Earnings Forecast Properties

Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)

	(1)			
Variable	***WELLCAP***			
CYBER_EVENT	0.855***			
	(13.72)			
BTM	-0.082***			
	(-4.72)			
LEV	-3.706***			
	(-33.17)			
NIM	91.71***			
	(15.97)			
ASSET TANGIBILITY	-17.145***			
	(-8.81)			
NPAT	4.648***			
	(4.21)			
PLL	-96.425***			
	(-15.22)			
NCO	-161.303***			
	(-14.92)			
STOCK_TURNOVER	-0.112***			
	(-7.79)			
NUMANA	0.115***			
	(3.57)			
EXPOSURE	0.005***			
	(5.82)			
GENANA	0.345***			
	(27.74)			
INTERCEPT	4.272***			
	(30.46)			
Pseudo R2	0.3575			

Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)

	(1)	**(2)**	**(3)**	**(4)**
Variable	***REVISE***	***FERROR***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
WELLCAP (1 VS 0)	-0.059*	-0.0094***	-0.861***	-0.0179
	(-1.75)	(-5.46)	(-2.78)	(-0.55)

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

Table 12				
The Relation between Analyst Following Category and Individual Analyst Earnings Forecast Properties				
Panel A: First Stage of Propensity Score Matching (PSM) Analysis (Probit)				
	(1)			
Variable	***NUMANACAT***			
CYBER_EVENT	-0.436***			
	(-7.15)			
SIZE	1.304***			
	(83.55)			
BTM	0.148			
	(0.74)			
LEV	0.473***			
	(9.78)			
NIM	65.43***			
	(22.89)			
ASSET TANGIBILITY	-12.885***			
	(-11.81)			
CAPR1Q	-0.064***			
	(-18.28)			
CAPR2Q	-0.112***			
	(-26.08)			
NPAT	8.456***			
	(7.73)			
PLL	41.242***			
	(7.73)			
NCO	-17.248***			
	(-2.84)			
STOCK_TURNOVER	0.254***			
	(25.47)			
EXPOSURE	0.009***			
	(15.83)			
GENANA	-0.305***			
	(-31.55)			
INTERCEPT	-14.931***			
	(-110.67)			
Pseudo R2	0.5729			
Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation)				
	(1)	**(2)**	**(3)**	**(4)**
Variable	***REVISE***	***FERROR***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
NUMANACAT (1 VS 0)	0.083***	-0.0004*	-0.146	-0.189***
	(2.32)	(-1.64)	(-0.64)	(-17.94)
*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.				

Table 13

The Relation between Types of Cyber Events and Individual Analyst Earnings Forecast Properties for banks that Suffer Security Breaches

Panel A: First Stage of Propensity Score Matching (PSM) Analysis				
	(1)	**(2)**	**(3)**	
Variable	***CONFIDENTIALITY***	***AVAILABILITY***	***INTEGRITY***	
SIZE	-0.04*	-0.108**	0.071**	
	(-1.79)	(-2.49)	(2.07)	
BTM	0.157***	-0.758***	-0.249***	
	(2.87)	(-5.52)	(-3.26)	
LEV	0.469**	-1.418***	-0.078	
	(2.25)	(-3.3)	(-0.25)	
NIM	-4.447	11.562	-83.33***	
	(-0.95)	(1.34)	(-4.11)	
ASSET_TANGIBILITY	3.882	36.606***	-15.428***	
	(0.99)	(5.35)	(-2.85)	
CAPR1Q	0.133***	-0.116***	-0.06**	
	(8.38)	(-3.35)	(-2.46)	
CAPR2Q	-0.119***	-0.18***	0.107***	
	(-4.73)	(-2.99)	(2.99)	
NPAT	-26.375***	27.859***	32.264***	
	(-9.89)	(6.2)	(9.6)	
PLL	10.858	-162.739****	-157.07***	
	(0.77)	(-3.29)	(-5.75)	
NCO	-116.792***	-51.025	-61.266*	
	(-5.62)	(-1.00)	(-1.92)	
DAMAGE	-0.00042***		0.006***	
	(-5.00)		(6.3)	
AFFECTED_COUNT	-0.0000007***	-0.0000006**	-0.00001**	
	(-6.01)	(-2.14)	(-2.16)	
NUMANA	-0.456***	2.192***	0.626***	
	(-6.33)	(12.89)	(5.63)	
EXPOSURE	0.002	0.002	-0.0046***	
	(1.46)	(0.82)	(-3.05)	
INTERCEPT	1.043***	-4.702***	-2.534***	
	(4.22)	(-7.53)	(-6.46)	
Pseudo R2	0.0677	0.1985	0.0867	
Panel B: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation) with Confidentiality as Treatment				
	(1)	**(2)**	**(3)**	**(4)**
Variable	***FERROR***	***DISP***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
CONFIDENTIALITY (1 VS 0)	0.00043**	-0.024**	0.109	-0.116***
	(2.2)	(-2.29)	(0.92)	(-10.07)
SIZE	0.00024***	0.009*	0.321***	-0.018***
	(2.64)	(1.93)	(5.21)	(-2.92)
BTM	0.0051***	0.239***	-0.705***	-0.0009
	(24.86)	(22.62)	(-5.03)	(-0.06)

LEV	0.0052***	0.3***	2.575***	-0.157***
	(5.98)	(6.66)	(4.3)	(-2.69)
NIM	-0.031**	-2.55***	-85.011***	4.678***
	(-2.33)	(-3.67)	(-9.21)	(5.2)
ASSET_TANGIBILITY	0.14***	5.489***	50.799***	2.921***
	(8.47)	(6.4)	(4.46)	(2.63)
CAPR1Q	-0.00006	0.0019	0.391***	-0.0027
	(-0.93)	(0.62)	(9.37)	(-0.67)
CAPR2Q	0.0001	-0.0037	-0.174**	0.021***
	(0.97)	(-0.68)	(-2.39)	(2.89)
NPAT	0.02*	0.226	5.251	2.477***
	(1.81)	(0.4)	(0.7)	(3.36)
PLL	0.65***	72.44***	97.712***	3.587
	(14.2)	(30.48)	(3.09)	(1.16)
NCO	0.389***	28.734***	9.993	22.502***
	(5.71)	(8.13)	(0.21)	(4.91)
DAMAGE	-0.0000002	-0.00005	-0.0007	0.0005***
	(-0.14)	(-0.87)	(-0.85)	(7.27)
AFFECTED_COUNT	0.000000002***	0.00000002	0.0000003	-0.0000003***
	(3.64)	(0.7)	(0.93)	(-9.07)
NUMANA	-0.0037***	-0.116***	-1.835***	-0.0082
	(-12.8)	(-7.67)	(-9.15)	(-0.42)
EXPOSURE	0.000014***	0.0007***	0.005*	-0.0009***
	(2.94)	(3.02)	(1.66)	(-2.99)
INTERCEPT	0.0015	-0.111**	-2.578***	0.863***
	(1.48)	(-2.16)	(-3.79)	(13.02)
Adjusted R2	0.2494	0.3695	0.0750	0.0990
Panel C: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation) with Availability as Treatment				
	(1)	**(2)**	**(3)**	**(4)**
Variable	***FERROR***	***DISP***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
AVAILABILITY (1 VS 0)	0.0064***	-0.052***	0.961***	-0.122***
	(8.22)	(-13.89)	(22.41)	(-17.52)
SIZE	0.00025**	0.015***	0.314***	-0.027***
	(2.38)	(2.75)	(4.00)	(-3.7)
BTM	0.0052***	0.237***	-0.79***	-0.015
	(22.13)	(19.32)	(-4.51)	(-0.93)
LEV	0.0054***	0.148***	3.295***	-0.103
	(5.32)	(2.76)	(4.33)	(-1.44)
NIM	-0.035**	-1.826**	-95.583***	4.844
	(-2.43)	(-2.41)	(-8.83)	(4.78)
ASSET_TANGIBILITY	0.143***	5.763***	63.638***	0.257
	(7.39)	(5.64)	(4.36)	(0.19)
CAPR1Q	0.00001	0.003	0.446***	-0.007
	(0.15)	(0.86)	(8.73)	(-1.47)
CAPR2Q	0.00013	0.005	-0.203**	0.031***

	(1.07)	(0.78)	(-2.24)	(3.67)
NPAT	0.023*	-0.477	7.5	2.787***
	(1.81)	(-0.73)	(0.8)	(3.18)
PLL	0.522***	71.181***	-113.038***	7.717**
	(10.65)	(27.57)	(-3.07)	(2.24)
NCO	0.284***	22.687***	-184.43***	26.32***
	(3.95)	(5.99)	(-3.41)	(5.2)
AFFECTED_COUNT	0.000000002***	0.00000002	0.000003	-0.0000003***
	(3.33)	(0.88)	(0.8)	(-6.69)
NUMANA	-0.0045***	-0.112***	-2.088***	0.018
	(-13.51)	(-6.44)	(-8.39)	(0.76)
EXPOSURE	0.000008	0.0006**	0.0046	-0.00045
	(1.54)	(2.32)	(1.18)	(-1.24)
INTERCEPT	0.0031***	-0.179***	-2.552***	0.816***
	(2.8)	(-3.07)	(-3.06)	(10.46)
Adjusted R2	0.2548	0.3763	0.0844	0.0746
Panel D: Second Stage of Propensity Score Matching (PSM) Analysis (Estimation) with Integrity as Treatment				
	(1)	**(2)**	**(3)**	**(4)**
Variable	***FERROR***	***DISP***	***UNCERTAINTY***	***INFORMATION ASYMMETRY***
INTEGRITY (1 VS 0)	-0.00093***	-0.012	-0.607***	0.155***
	(-5.43)	(-1.21)	(-12.27)	(8.85)
SIZE	0.00024**	0.0128**	0.26***	-0.0032
	(2.53)	(2.48)	(3.62)	(-0.48)
BTM	0.0049***	0.217***	-0.856***	0.01
	(23,40)	(18.94)	(-5.35)	(0.67)
LEV	0.0056***	0.285***	3.242***	-0.245***
	(5.97)	(5.57)	(4.55)	(-3.64)
NIM	-0.033**	-2.004***	-99.932***	5.852***
	(-2.46)	(-2.7)	(-9.67)	(5.99)
ASSET_TANGIBILITY	0.146***	5.809***	52.737***	3.261***
	(8.47)	(6.17)	(4.02)	(2.63)
CAPR1Q	-0.000008	-0.0005	0.467***	-0.0084*
	(-0.13)	(-0.13)	(9.54)	(-1.82)
CAPR2Q	0.00025**	-0.002	-0.164*	0.0138*
	(2.29)	(-0.33)	(-1.96)	(1.74)
NPAT	0.022**	0.757	4.434	3.723***
	(2.07)	(1.27)	(0.54)	(4.76)
PLL	0.484***	71.856***	-146.447***	11.644***
	(10.43)	(28.3)	(-4.14)	(3.48)
NCO	0.274***	31.934***	-225.997***	34.384***
	(4.13)	(8.79)	(-4.47)	(7.19)
DAMAGE	0.000002	-0.000006	0.00022	0.0006***
	(1.38)	(-0.95)	(0.25)	(7.43)
AFFECTED_COUNT	0.000000002***	0.00000003	0.0000003	-0.0000003***
	(3.36)	(1.12)	(0.64)	(-6.6)
NUMANA	-0.004***	-0.124***	-1.92***	-0.029

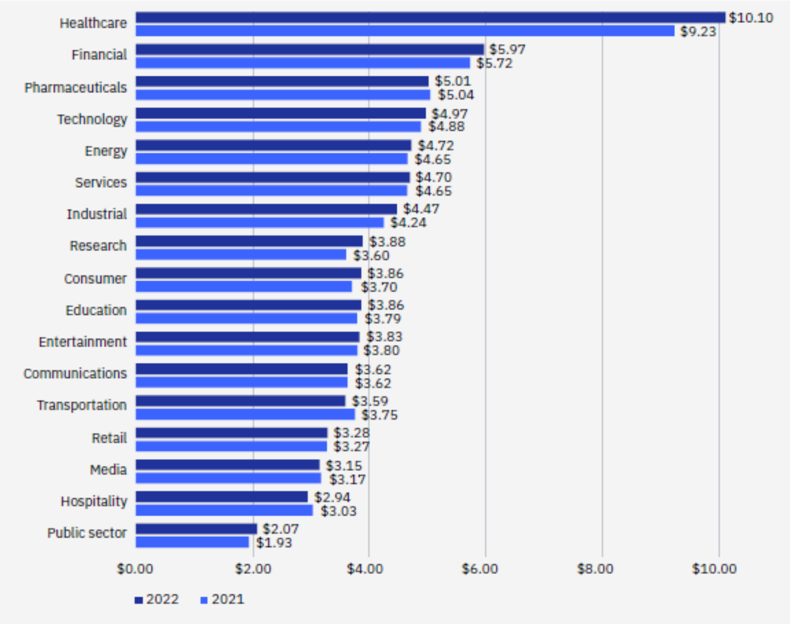
	(-13.5)	(-7.52)	(-8.38)	(-1.32)
EXPOSURE	0.000009*	0.00071***	0.0052	-0.0004
	(1.89)	(2.72)	(1.43)	(-1.29)
INTERCEPT	0.0021**	-0.12**	-2.374***	0.699***
	(2.1)	(-2.17)	(-3.09)	(9.61)
Adjusted R2	0.2671	0.3603	0.0938	0.1128

*, **, *** Indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

FIGURES

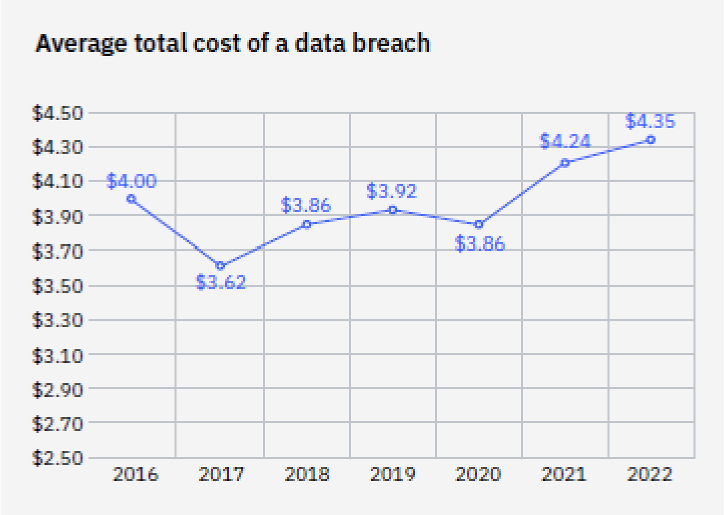
Figure 1: Average Cost of Data Breach by Industry in 2022

(Measured in USD million)



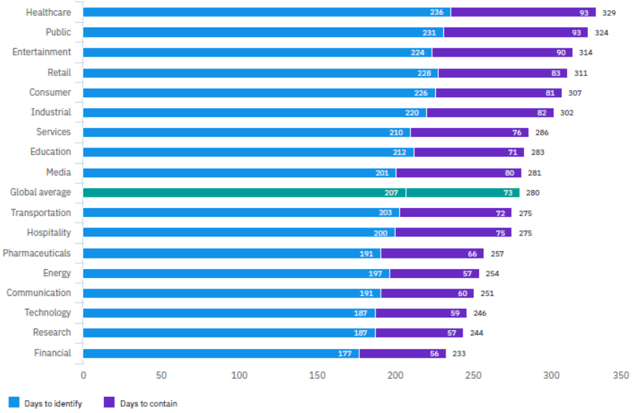
(IBM Security, 2022)

Figure 2: Average Total Cost of a Data Breach in 2022 (Measured in USD million)



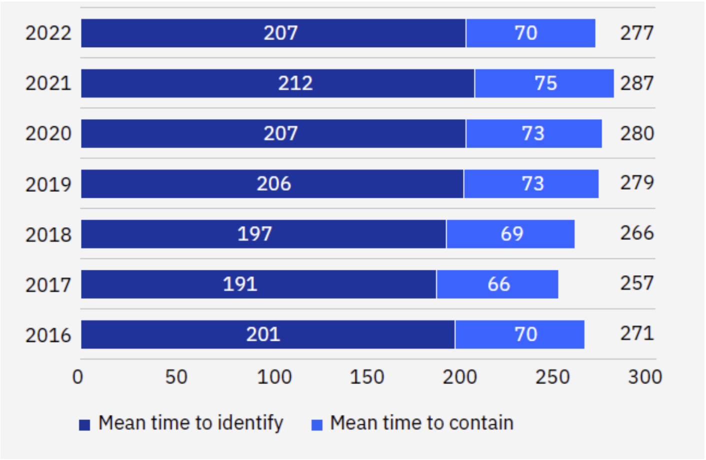
(IBM Security, 2022)

Figure 3: Days to Identify and Contain a Data Breach by Industry Sector in 2020 (Measured in days)



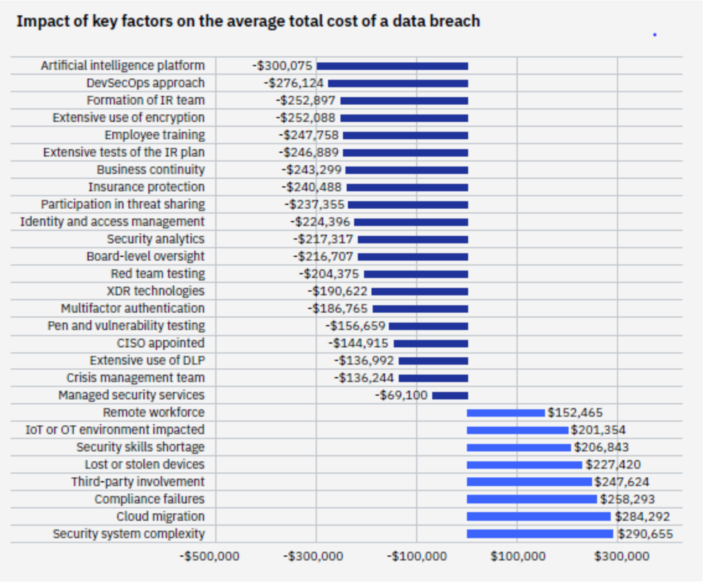
(IBM Security, 2020)

Figure 4: Days to Identify and Contain a Data Breach by Industry Sector in 2022 (Measured in days)



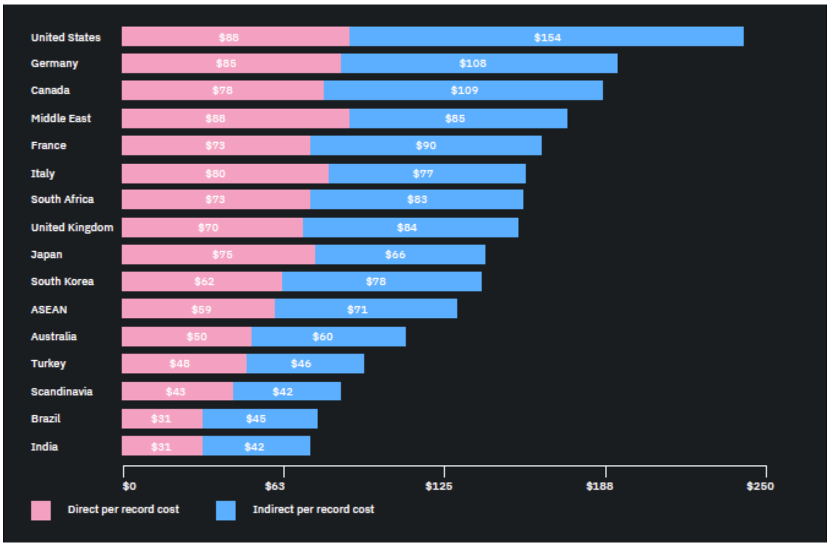
(IBM Security, 2022)

Figure 5: Impact of Key Factors on the Average Cost of the Data Breach in 2022 (Measured in USD)



(IBM Security, 2022)

Figure 6: Direct and Indirect Costs by Country or Region (Measured in USD)



(IBM Security, 2019)

Figure 7: Financial Analysts Earnings Forecast after Security Breaches during Quarter *t*.

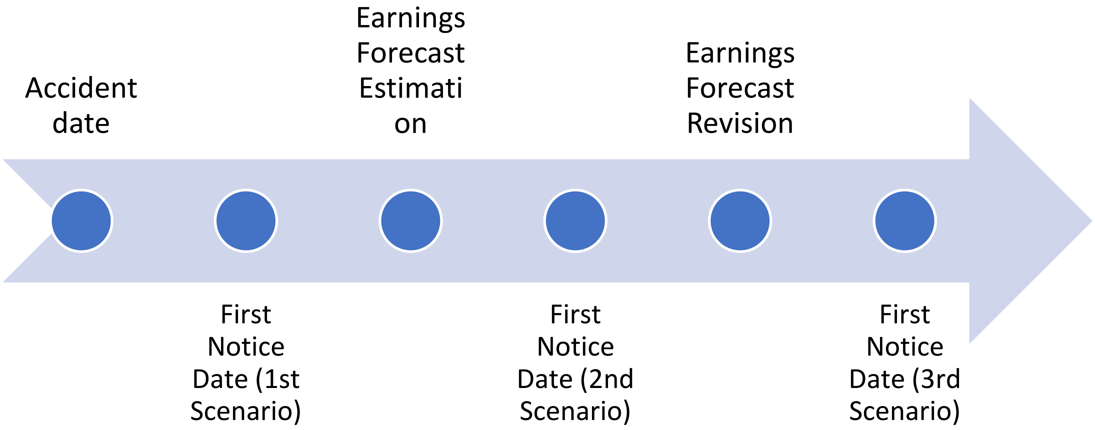
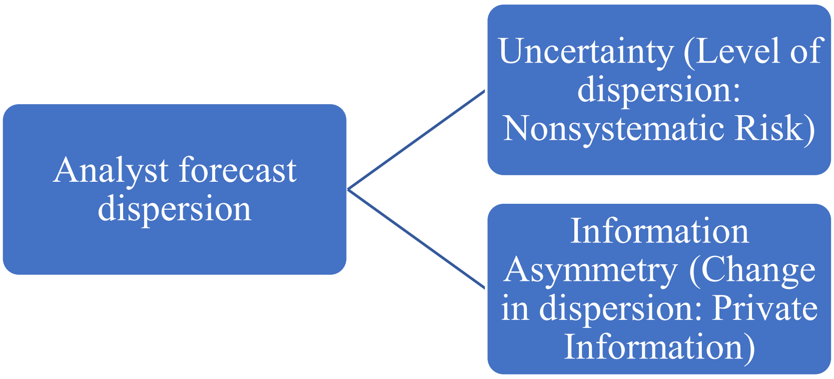

Accident date
Earnings Forecast Estimati on
Earnings Forecast Revision
First Notice Date (1st Scenario)
First Notice Date (2nd Scenario)
First Notice Date (3rd Scenario)

Figure 8: A Diagram of How Uncertainty and Information Asymmetry among Financial Analysts Interrelate


Analyst forecast dispersion
Uncertainty (Level of dispersion: Nonsystematic Risk)
Information Asymmetry (Change in dispersion: Private Information)

References

Acquisti, A. (2004). Privacy and security of personal information: Economic incentives and technological solutions. *Economics of Information Security*, 179-186.

Ali, A., Liu, M., Xu, D., & Yao, T. (2019). Corporate disclosure, analyst forecast dispersion, and stock returns. *Journal of Accounting, Auditing & Finance*, 34(1), 54-73.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), 1177-1206.

Ayres, D., Huang, X. S., & Myring, M. (2017). Fair value accounting and analyst forecast accuracy. *Advances in Accounting*, 37, 58-70.

Barniv, R. R., & Cao, J. (2009). Does information uncertainty affect investors' responses to analysts' forecast revisions? An investigation of accounting restatements. *Journal of Accounting and Public Policy*, 28(4), 328-348.

Barron, O. E., Kim, O., Lim, S. C., & Stevens, D. E. (1998). Using analysts' forecasts to measure properties of analysts' information environment. *The Accounting Review*, 421-433.

Barron, O. E., Stanford, M. H., & Yu, Y. (2009). Further evidence on the relation between analysts' forecast dispersion and stock returns. *Contemporary Accounting Research*, 26(2), 329-357.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508-526.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, 37(6), 527-544.

Bouveret, A. (2018). *Cyber risk for the financial sector: a framework for quantitative assessment.* International Monetary Fund.

Bradshaw, M., Ertimur, Y., & O'Brien, P. (2017). Financial analysts and their contribution to well-functioning capital markets. *Foundations and Trends in Accounting*, 11(3), 119-191.

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, 19(1), 396-455.

Campbell, J. L., Twedt, B. J., & Whipple, B. C. (2021). Trading Prior to the Disclosure of Material Information: Evidence from Regulation Fair Disclosure Form 8-Ks. *Contemporary Accounting Research*, 38(1), 412-442.

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

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

Coën, A., Desfleurs, A., & L'Her, J. F. (2009). International evidence on the relative importance of the determinants of earnings forecast accuracy. *Journal of Economics and Business*, 61(6), 453-471.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, 37(6), 564-585.

Factset Callstreet (2014, January). *JP Morgan Chase & Co. Q4 2013 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2014, October). *Bank of America Corp. Q3 2014 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2014, October). *Capital One Financial Corp. Q3 2014 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2014, October). *Citigroup, Inc. Q3 2014 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2015, July). *Capital One Financial Corp. Q2 2015 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2016, July). *JP Morgan Chase & Co. Q2 2016 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2016, October). *Bank of America Corp. Q3 2016 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2016, October). *The Bank of New York Mellon Corp. Q3 2016 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2017, January). *Bank of America Corp. Q4 2016 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2017, January). *JP Morgan Chase & Co. Q4 2016 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2017, October). *Citigroup, Inc. Q3 2017 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2018, April). *Citigroup, Inc. Q1 2018 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2018, January). *The Bank of New York Mellon Corp. Q4 2017 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2019, April). *JP Morgan Chase & Co. Q1 2019 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2019, January). *Capital One Financial Corp. Q4 2018 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2019, July). *Citigroup, Inc. Q2 2019 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2019, October). *Capital One Financial Corp. Q3 2019 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2019, October). *Citigroup, Inc. Q3 2019 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2020, January). *Citigroup, Inc. Q4 2019 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2021, January). *JP Morgan Chase & Co. Q4 2020 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2022, April). *Citigroup, Inc. Q1 2022 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Factset Callstreet (2022, April). *JP Morgan Chase & Co. Q1 2022 Earnings Call* (Corrected Transcript). Retrieved from Factset database.

Fazzini, K. (2018). Moody’s Is Going to Start Building the Risk of a Business-Ending Hack into Its Credit Ratings.

Filzen, J. J. (2015). The information content of risk factor disclosures in quarterly reports. *Accounting Horizons*, 29(4), 887-916.

Filzen, J. J., McBrayer, G. A., & Shannon, K. S. (2023). Risk factor disclosures: do managers and markets speak the same language? *Accounting Horizons*, 1-17.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6), 461-485.

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

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5), 503-530.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808-834.

Hausken, K. (2006), "Income, interdependence, and substitution effects affecting incentives for security investment", *Journal of Accounting and Public Policy*, 25(6), 629-665.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6), 639-688.

Havakhor, T., Rahman, M. S., & Zhang, T. (2020). Cybersecurity investments and the cost of capital. *SSRN Electronic Journal*.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, 30(3), 79-98.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? *Georgetown McDonough School of Business Research Paper*, (2852519).

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6(2), 97–121.

Hovav, A., & D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. *Information Systems Security*, 13(3), 32–40.

Hovav, A., & D'arcy, J. (2005). Capital market reaction to defective IT products: The case of computer viruses. *Computers & Security*, 24(5), 409-424.

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

IBM Security: *Cost of data breach report* (2019). [PDF file]. Retrieved from https://www.ibm.com/security/data-breach.

IBM Security: *Cost of data breach report* (2020). [PDF file]. Retrieved from https://www.ibm.com/security/data-breach.

IBM Security: *Cost of data breach report* (2022). [PDF file]. Retrieved from https://www.ibm.com/security/data-breach.

Identity Theft Resource Center (ITRC): *End-of-year data breach report* (2018). [PDF file]. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

Jung, M. J., Wong, M. F., & Zhang, X. F. (2018). Buy-side analysts and earnings conference calls. Journal of Accounting Research, 56(3), 913-952.

Koch, A. S., Lefanowicz, C. E., & Robinson, J. R. (2013). Regulation FD: A review and synthesis of the academic literature. Accounting Horizons, 27(3), 619-646.

Kravet, T., Muslu, V. (2013). Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies*, 18(4), 1088–1122.

Kross, W. J., & Suk, I. (2012). Does Regulation FD work? Evidence from analysts' reliance on public disclosure. Journal of Accounting and Economics, 53(1-2), 225-248.

Kwon, J., and Johnson, M. E. (2013). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems* 30(2), 41-66.

Kwon, J., and Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector, *MIS Quarterly* 38(2), 451-471.

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

Leeson, P. T., and Coyne, C. J. (2005). The Economics of Computer Hacking. *Journal of Law, Economics and Policy*, 1(2), 511-532.

Lehavy, R., Li, F., & Merkley, K. (2011). The effect of annual report readability on analyst following and the properties of their earnings forecasts. *The Accounting Review*, 86(3), 1087-1115.

Leung, R. (2018). Cybersecurity regulation in the banking sector: Global emerging themes. The London School of Economics and Political Science.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, 40-55.

Liu, C., & O'Farrell, G. (2013). The role of accounting values in the relation between XBRL and forecast accuracy. *International Journal of Accounting and Information Management*

Liu, X. G., & Natarajan, R. (2012). The effect of financial analysts' strategic behavior on analysts' forecast dispersion. *The Accounting Review*, 87(6), 2123-2149.

Lu, C. W., Chen, T. K., & Liao, H. H. (2010). Information uncertainty, information asymmetry and corporate bond yield spreads. Journal of Banking & Finance, 34(9), 2265-2279.

Ramnath, S., Rock, S., & Shane, P. (2008). The financial analyst forecasting literature: A taxonomy with suggestions for further research. *International Journal of Forecasting*, 24(1), 34-75.

Securities and Exchange Commission (SEC) (2011), “CF Disclosure Guidance: Topic No. 2”, available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Securities and Exchange Commission (SEC) (2018), “Commission statement and guidance on public company cybersecurity disclosures”, available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Tan, H., Wang, S., & Welker, M. (2011). Analyst following and forecast accuracy after mandated IFRS adoptions. *Journal of Accounting Research*, 49(5), 1307-1357.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005), “Vulnerability and information security investment: an empirical analysis of E-local government in Japan”, *Journal of Accounting and Public Policy*, 24(1), 37-59.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, 33(8), 544-557.

The innovation journey: Eyes on execution: Cybersecurity. (n.d.). Retrieved from https://www.pwc.com/ca/en/banking-capital-markets/assets/pwc-industries-fs-canadianbanks2018-cybersecurity-EN.pdf.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309.

Yoon, H., Zo, H., & Ciganek, A. P. (2011). Does XBRL adoption reduce information asymmetry?. *Journal of Business Research*, 64(2), 157-163.

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers,* 18(6), 1205-1215.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal*, 25(1), 21-37.

Zhang, X. F. (2006). Information uncertainty and analyst forecast behavior. *Contemporary Accounting Research*, 23(2), 565-590.