Journal of Global Business Insights

Volume 8 | Issue 2 Article 3

September 2023

An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States

Asligul Erkan-Barlow
East Carolina University, erkana18@ecu.edu

Thanh Ngo
East Carolina University, ngot@ecu.edu

Rajni Goel
Howard University, rgoel@howard.edu

See next page for additional authors

Recommended Citation

Erkan-Barlow, A., Ngo, T., Goel, R., & Streeter, D. W. (2023). An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States. *Journal of Global Business Insights, 8*(2), 120-135. https://www.doi.org/10.5038/2640-6489.8.2.1246

An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States

Authors

Asligul Erkan-Barlow, Thanh Ngo, Rajni Goel, and Denise W. Streeter

Corresponding Author

Asligul Erkan-Barlow, 102 Oak Towne Drive, Unit A6 , Greenville, NC 27858

Abstract

This study examined the effects of cyberattacks on the profitability of U.S. public and private commercial banks using a sample of 120 data breaches across various institutions. The results showed that cyberattacks negatively influence bank profitability, with effects more robust in the 12 quarters following a breach, especially from non-hack breaches. Large and private banks suffer more than small and public banks, with breaches resulting in decreased deposits and loans and increased liquidity. These changes are confirmed as independent channels reducing bank profitability. The results were robust after controlling for factors like multicollinearity, non-stationarity, cross-sectional dependence, and heteroskedasticity.

Keywords

cybersecurity, data breaches, breach types, performance ownership

Revisions

Submission date: Jul. 22, 2022; 1st Revision: Nov. 5, 2022; 2nd Revision: Mar. 15, 2023; 3rd Revision: Aug. 24, 2023; Acceptance: August 30, 2023

An In-Depth Analysis of the Impact of Cyberattacks on the Profitability of Commercial Banks in the United States

Asligul Erkan-Barlow[1], Thanh Ngo[2], Rajni Goel[3], and Denise W. Streeter[4]

The College of Business
East Carolina University, United States
[1]erkana18@ecu.edu
[2]ngot@ecu.edu

The School of Business
Howard University, United States
[3]rgoel@howard.edu
[4]denise.streeter@howard.edu

Abstract

This study examined the effects of cyberattacks on the profitability of U.S. public and private commercial banks using a sample of 120 data breaches across various institutions. The results showed that cyberattacks negatively influence bank profitability, with effects more robust in the 12 quarters following a breach, especially from non-hack breaches. Large and private banks suffer more than small and public banks, with breaches resulting in decreased deposits and loans and increased liquidity. These changes are confirmed as independent channels reducing bank profitability. The results were robust after controlling for factors like multicollinearity, non-stationarity, cross-sectional dependence, and heteroskedasticity.

Keywords: cybersecurity, data breaches, breach types, performance ownership

Introduction

According to Statista (2022), data breaches have increased notably with cybersecurity costs rising from $27.4 billion in 2010 to $60.4 billion in 2017. These breaches concern financial services firms which face up to 300 times more attacks per year (Zakrzewski et al., 2019). Since financial institutions, especially banks, are the backbone of the financial system, this research aimed to study the economics of data breaches at commercial banks. Specifically, we sought to estimate the performance implications of cyberattacks experienced by U.S. commercial banks and to understand the channels through which their profitability is affected.

The existing literature examining the impacts of cybersecurity incidents shows that these adverse events can cause significant damage to firms, the public, and the financial ecosystem. Data breaches generally cause interruptions in firm operations (Gordon et al., 2011) and result in declining sales growth, credit ratings, and risk appetite (Kamiya et al., 2021). Firms that experience unauthorized access to their computer networks face financial and reputational damage, litigation,

and attorney costs (Garg, 2020). Cyberattacks in the financial services industry can destabilize the financial sector by causing a wider-scale disruption due to the interconnectedness of the financial system (Kashyap & Wetherilt, 2019). Understanding the performance consequences of cyberattacks on commercial banks is highly important since these institutions are the intermediaries between investors and industries. Any adverse impact on their profitability can potentially hinder economic stability and growth in a country (Christaria & Kurnia, 2016).

Cyber incidents might reduce the profitability of commercial banks. Data breaches may increase operating costs as they experience damage to technological assets and service interruptions. The negligence and disruptions in bank operations following cyberattacks deteriorate customers' confidence in their banks (Bouveret, 2018). As a corollary, banks can experience cyber runs on deposits when unsatisfied customers withdraw their existing deposits or stop processing new ones once they encounter account access problems (Duffie & Younger, 2019). Lending et al. (2018), for example, documented a significant decrease in bank deposits following a cyberattack. According to *the idiosyncratic viral loss theory*, unexpected events might harm the affected firm and the economy in which it operates, including banks and the financial services industry (Velez, 2021). However*, the theory of the firm* suggests that cyberattacks might not have performance consequences. According to this theory, firms exist to improve and maintain profitability (Jensen & Meckling, 1976). Consistent with this prediction, empirical evidence documents a marginal decline in profitability for large firms only (Kamiya et al., 2021) and only in the third quarter following a breach (Ko & Dorantes, 2006). Banks must continue their lending roles as financial intermediaries, even if this requires assistance when they face liquidity problems (Kashyap & Stein, 2000). Thus, breached banks might experience a decline in deposits without having a severe impact on their profitability due to operational adjustments. This study aimed to reconcile these competing views by examining the performance implications of cyberattacks on U.S. commercial banks.

We further explored if different structures influence the relationship between data breaches and bank profitability. Prior research establishes that the impact of data breaches on the value and operations of a firm may vary by breach type. Existing studies document a significant adverse market reaction to breach announcements only when the incident involves unauthorized access to confidential data (Campbell et al., 2003) or when it affects the availability of information (Gordon et al., 2011). The size and ownership of banks may also influence this relationship, with larger institutions handling cyber incidents better (Cavusoglu et al., 2004), while small, medium-sized, and private banks may struggle due to limited resources (Barry et al., 2011; Servidio et al., 2015). Understanding the impact on these institutions is crucial, as performance failures could affect customers and communities. Finally, we identified bank deposits (Lending et al., 2018), bank lending (Kashyap & Stein, 2000), and bank liquidity (Duffie & Younger, 2019) as the channels affecting the profitability of commercial banks. Our study controls possible causality among these three channels. We addressed three key questions:

1. How do cyberattacks affect U.S. commercial banks' profitability?
2. How do factors like breach type, bank size, and ownership influence this relationship?
3. Through what channels do data breaches impact profitability?

This study contributes to different strands of literature, theory, and practice. First, our study was the first to extensively explore the influence of data breaches on both publicly traded and privately owned U.S. commercial banks. We broadened the scope of research in this area, providing

empirical evidence that is inclusive of different banking structures, thereby enhancing the generalizability and practical relevance of the findings. Second, we introduced a novel examination of the specific channels (deposits, lending, and liquidity) through which data breaches affect commercial the profitability of commercial banks, offering a more nuanced insight into the operational consequences of cyber incidents. Third, we extended the idiosyncratic viral loss theory by providing data breaches as a new example of an unexpected event that may interrupt firm operations and hinder performance.

Our findings carry significant implications for various stakeholders in the banking industry. We highlighted that non-hack breaches are more detrimental to commercial bank performance, suggesting that banks should prioritize preventing these incidents. The delayed effect of data breaches, taking two to three years to manifest, emphasizes the need for long-term vigilance by bank managers. Additionally, our research showed larger and privately owned banks are more vulnerable to cyberattacks, indicating the need for increased cybersecurity efforts in these institutions. Our research also contributed to the practice by providing evidence for the stronger negative impact of cyberattacks on larger and privately owned banks through specific channels, including customer trust and lending activities. This understanding equips bank managers to try to restore trust to prevent declines in customer deposits and continue their lending activities to maintain profitability. These findings have practical implications for individual bank customers and businesses as they might be better off working with smaller banks, especially when they seek debt financing.

Our study also has policy implications. Commercial banks are the backbones of a healthy economy, and any threat to their profitability risks the entire financial system. They contribute to industrial growth and job creation. The Federal Reserve Bank and regulatory authorities such as the Securities Exchange Commission and the Financial Industry Regulatory Authority should be sensitive to cybersecurity to prevent any negative economic impact. The Federal Reserve Bank could provide extended support to breached banks, and regulatory agencies could provide specific guidelines to assist banks in developing and maintaining security practices.

Literature Review

Impact of Data Breaches on Bank Profitability

Cyberattacks affect firms negatively in various ways. Studies show that such attacks lead to negative stock price reactions and significant declines in market values (Campbell et al., 2003; Cavusoglu et al., 2004; Gordon et al., 2011). Some findings suggest a wealth loss within one month of a data breach (Iyer et al., 2020), but the negative impact on profitability may only manifest in the third quarter following a breach or may affect only large firms (Kamiya et al., 2021; Ko & Dorantes, 2006). This aligns with the theory that firms operate to maximize profits, so cyberattacks may not necessarily harm profitability (Jensen & Meckling, 1976). In contrast, cyberattacks may have severe implications for financial institutions and the financial system's stability (Christaria & Kurnia, 2016). The potential fallout includes operational disruptions, loss of revenue and customer relationships, and increased insurance premiums (Garg, 2020). Kashyap and Wetherilt (2019) argued that cyber incidents are different from other exogenous shocks because the interconnectedness of the financial system causes a wider-scale disruption. Eisenbach et al. (2021) showed that a cyberattack on one of the top five banks might impair one-third of the entire network.

The idiosyncratic viral loss theory states that unexpected events will occur and impact the related firm or even the entire economy in which it operates. The theory derives its name from unpredictable viruses, which spread fast and may have global impacts. Velez (2021) argued that idiosyncratic viral losses are significant threats to the financial services industry. As low-frequency, high-severity events that are hard to quantify (Eling & Zhu, 2018), we propose that data breaches may impact the profitability of banks by interrupting their operations and creating new expenses.

- Hypothesis 1: Experiencing a data breach negatively influences bank profitability.

Breach Type

After establishing a direct relationship between experiencing a data breach and profitability, we explore our second research question. Campbell et al. (2003) find negative market reactions mainly to breaches involving unauthorized access, especially those initiated by employees. Gordon et al. (2011) focus on breaches affecting information availability, while Kamiya et al. (2021) define data breaches as cyberattacks involving the loss of personal financial information. Similarly, we suspect that the impact of a cyber incident on a bank's performance may vary by the breach type. We categorize breaches into two groups, HACK - hacks by an outside party or infected by malware and NON-HACK - all remaining breach events. Outside parties might not have as much information about firms' security systems. Thus, the external hacks might have fewer damaging effects than those penetrating from the inside parties, who might have direct or easier access to proprietary information. Alternatively, hacks by outside parties might be larger in magnitude compared to incidents caused by inside parties. Company insiders might want to disguise their identity and maintain their employment. Thus, they might not trigger a major incident to avoid being detected. Similarly, information security failures that stem from lost or stolen devices might be smaller in scale compared to hacking incidents that might compromise the integrity of the entire security system.

- Hypothesis 2a: The negative influence of a data breach on a bank's profitability is stronger among NON-HACK breach events.
- Hypothesis 2b: The negative influence of a data breach on a bank's profitability is stronger among HACK breach events.

Bank Size

Data breaches affect banks of all sizes differently. Large institutions benefit from economies of scale, giving them advantages like greater access to capital markets and technical skills, enabling them to handle breaches more effectively (Cavusoglu et al., 2004). Conversely, small, and midsize banks often lack the resources to combat cyberattacks and may suffer more substantial negative impacts on profitability (Servidio et al., 2015). Thus, the negative impact of a data breach on a bank's profitability might be more substantial among smaller banks.

- Hypothesis 3: The negative influence of a data breach on a bank's profitability is stronger among smaller banks than larger banks.

Bank Ownership

The bank ownership structure is a determinant of profitability often overlooked. Earlier studies document that management-controlled banks outperform owner-controlled banks (Vernon, 1971),

and multiple-bank holding companies outperform one-bank holding companies (Mullineaux, 1978). More recently, Barry et al. (2011) show that public banks have greater access to financial markets and raise equity capital at a lower cost. Having access to limited capital, private banks may have fewer resources to allocate to cybersecurity so they may suffer more severe consequences after a cyberattack. In contrast, *the agency theory* suggests that agency conflicts that stem from the separation of ownership and control in publicly traded institutions do not apply to private institutions (Jensen & Meckling, 1976). Barry et al. (2011) argue that private banks' shareholders experience less information asymmetry. Authors posit that private banks rely heavily on debt financing, associated with more robust monitoring through loan covenants. Kwan (2004) also documents that larger bank-holding companies are less profitable than their privately owned peers. Thus, private banks may absorb the negative consequences of data breaches more easily than publicly traded banks.

- Hypothesis 4a: The negative influence of a data breach on a bank's profitability is stronger among privately owned banks.
- Hypothesis 4b: The negative influence of a data breach on a bank's profitability is stronger among publicly traded banks.

Channels Through Which Data Breaches Impact Banks' Profitability

Bank Deposits

This study also identifies three channels through which cyberattacks may influence commercial banks' profitability to address our third research question. Deposits, as one of these channels, capture the response of a bank's customers to adverse situations. Interruptions in payment systems erode customer trust (Bouveret, 2018), leading to around a 10% decline in deposits (Lending et al., 2018) and decreased growth rates in small U.S. banks (Gogolin et al., 2021). Loss of confidence may further cause cyber runs on deposits, reducing profitability (Duffie & Younger, 2019). Thus, data breaches might impact banks' profitability by causing a decrease in their deposits.

- Hypothesis 5: The decrease in bank deposits is the channel through which a data breach negatively influences a bank's profitability.

Bank Lending

Lending is another key factor in bank profitability, separate from deposits, and essential for maintaining profitability. Net interest margin, a standard proxy for performance, measures the gap between interest paid to depositors and received from borrowers, highlighting the distinct roles of deposits and loans (Chen et al., 2018). Kashyap and Stein (2000) suggest that banks with less liquid balance sheets should be stimulated with monetary policy to continue in their lending role, which implies that loans may not always be directly associated with deposits. We argue that banks may decrease their lending after a breach to direct funds to other functions, regardless of the change in customer deposits. Thus, breaches may negatively influence a bank's profitability by causing a decline in its lending after controlling for possible changes in bank deposits.

- Hypothesis 6: The decrease in bank lending is the channel through which a data breach negatively influences a bank's profitability.

Bank Liquidity

Finally, bank liquidity is another determinant of bank performance, and cyberattacks can have complex effects on it. Attacks can erode trust, potentially triggering a cyber run-on bank and decreasing liquidity (Bouveret, 2018; Duffie & Younger, 2019). In contrast, breached banks may increase liquidity to prepare for unforeseen expenses like informing customers, public image restoration, and legal fees (Garg, 2020). If breached banks adopt policies similar to those of breached non-bank organizations, they might also increase their liquidity levels to prepare for unforeseen expenses that may arise in the future. Nevertheless, higher liquidity levels may have severe performance consequences. Chen et al. (2018) report a negative association between a bank's liquidity and profitability due to the higher cost of obtaining liquidity. As a result, a breach may negatively impact a bank's profitability due to the increase in liquidity.

- Hypothesis 7: The increase in bank liquidity is the channel through which a data breach negatively influences a bank's profitability.

Methods

Data Sources

We follow recent studies (Garg, 2020; Kamiya et al., 2021; Lending et al., 2018) and utilize the Privacy Rights Clearinghouse (PRC) database to identify the breach incidents in our sample. The website provides comprehensive information on 9,015 cyber events made public in the U.S. from 2005 through 2019. In addition to the PRC, we use the SNL Financial–Regulated Depositories dataset to obtain the financial statement information on banks. This dataset includes data from Credit Union and Corporate Credit Union Financials (5300, 5310), Small and Large Parent Company Financials (Y-9LP, Y-9SP), as well as Holding Companies Financials (Y-9C) and Call Report Financials (031, 041, 051). Employing this database allows us to be consistent with Lending et al. (2018), who retrieved information from the Consolidated Financial Statements for Holding Companies (FR Y-9C) form.

Sample Construction

We employ a fuzzy name-matching procedure to match the PRC dataset with the SNL. We match 57% of the PRC breaches among banks to the SNL. We then manually check the names to ensure the quality of the match. For the remaining 43% of the PRC sample that cannot be matched using the fuzzy matching procedure, we manually match them one by one; 9% of which cannot be matched reliably which we remove from our sample. Our sample criteria also require accounting data availability for at least four out of 12 quarters before and after the incident, resulting in 120 incidents from 2005 to 2018. Unlike Lending et al. (2018) and Kamiya et al. (2021), our sample includes both publicly traded and privately held banks, extends to 2018 and focuses solely on banks. Our sample period extends to 2018, while Lending et al. (2018) stopped in 2012. We focus only on banks, while Kamiya et al. (2021) examine all financial institutions. Table 1 reports the distribution of the breached banks in our sample by year (Panel A), by breach type (Panel B), and by the public status of the banks (Panel C). Panel A shows that 2010 was the worst year for banks. Panel B identifies *Hacking or malware* (HACK) and *Insider* (INSD) as the most common types of cyber events that resulted in 30 and 25 incidents, respectively. Panel C portrays that 20 percent of our sample consists of private banks.

Entropy Balancing

Lending et al. (2018), Garg (2020), and Kamiya et al. (2021) use propensity score matching, keeping only the closest non-breached control firm for each breached firm, which can lead to biased estimates (Abadie & Imbens, 2007). Hainmueller (2012), using an entropy balancing procedure, adjusts inequalities between treatment and control firms. We identify 100 non-breached banks closest in assets to 120 breached banks, remove the breached ones for clear analysis, and apply the entropy balancing procedure to ensure that the distributions of bank characteristics are not significantly different between the groups. We examine characteristics such as LNASSET (the natural logarithm of bank assets at quarter t-1), DEPOSIT (the ratio of total deposits to total assets at quarter t-1), LOAN (the ratio of total loans to total assets at quarter t-1), NONPERLOAN (the percentage of nonperforming loans at quarter t-1), OPEREXP (the ratio of operating expenses to operating revenues at quarter t-1), and LIQUIDITY (the percentage of liquid assets to total asset at quarter t-1).

Table 1. Sample Distribution & Comparisons Before and After Entropy Balancing

Panel A – Breakout Year

Year	*N*	Percent
2005	4	3.33
2006	12	10.00
2007	6	5.00
2008	4	3.33
2009	5	4.17
2010	20	16.67
2011	12	10.00
2012	8	6.67
2013	17	14.17
2014	13	10.83
2015	6	5.00
2016	2	1.67
2017	5	4.17
2018	6	5.00
Total	120	100.00

Panel B – Type of Breach

Type	*N*	Percent
CARD	12	10.00
DISC	15	12.50
HACK	30	25.00
INSD	25	20.83
PHYS	4	3.33
PORT	17	14.17
STAT	3	2.50
UNKN	14	11.67
Total	120	100.00

Panel C – Public Status

Public Banks	96	80.00
Private Banks	24	20.00
Total	120	100.00

Panel D - Bank Characteristics Before Entropy Balancing

	Non-Breached Banks (*N* = 12,000)			Breached Banks (*N* = 120)			
Characteristic	Mean	Variance	Skewness	Mean	Variance	Skewness	Stdz. Diff.
$LNASSET_{t-1}$	16.5900	10.35000	0.04212	15.6700	4.59800	-0.4258	-0.429
$DEPOSIT_{t-1}$	0.6516	0.03557	-0.67880	0.7299	0.01784	-1.3140	0.586
$LOAN_{t-1}$	0.5888	0.03954	-0.43970	0.6336	0.02429	-0.9485	0.287
$NONPERLOAN_{t-1}$	2.2180	7.22000	2.53000	2.0250	6.38200	2.4650	-0.076
$OPEREXP_{t-1}$	62.0600	439.70000	0.14560	61.9200	277.30000	0.4043	-0.080
$LIQUIDITY_{t-1}$	0.3059	0.02605	0.85400	0.2736	0.02263	1.1030	-0.215

Panel E - Bank Characteristics After Entropy Balancing

	Non-Breached Banks (*N* = 12,000)			Breached Banks (*N* = 120)			
Characteristic	Mean	Variance	Skewness	Mean	Variance	Skewness	Stdz. Diff.
$LNASSET_{t-1}$	16.5900	10.35000	0.04212	16.5900	10.35000	-0.04212	0.000
$DEPOSIT_{t-1}$	0.6516	0.03557	-0.67880	0.6516	0.03557	-0.67880	0.000
$LOAN_{t-1}$	0.5888	0.03954	-0.43970	0.5888	0.03954	-0.43970	0.000
$NONPERLOAN_{t-1}$	2.2180	7.22000	2.53000	2.2180	7.22000	2.53000	0.000
$OPEREXP_{t-1}$	62.0600	439.70000	0.14560	62.0600	439.70000	0.14560	0.000
$LIQUIDITY_{t-1}$	0.3059	0.02605	0.85400	0.3059	0.02605	0.85400	0.000

We report the mean, variance, and skewness of the treatment and control banks before the implementation of the entropy balancing procedure in Panel D of Table 1. The standardized differences are calculated as the differences in the mean values of the characteristics between the two groups scaled by the standard deviation of the characteristics of the breached banks. Austin (2011) suggests that a standardized difference of less than 10% indicates a negligible difference in the mean of a characteristic between the treatment and control groups. The standardized

differences in NONPERLOAN and OPEREXP are 7.6% and 8%, respectively, but they are much larger than 10% in the LNASSET, DEPOSIT, LOAN, and LIQUIDITY. After the implementation of the entropy balancing procedure, the standardized differences in all control characteristics were reduced to 0% (see Panel E). Thus, any changes in the subsequent performance of the breached banks should be attributable to the breach events themselves instead of the bank characteristics.

Empirical Model

The difference-in-difference regression model is employed to estimate the differential impact of the treatment (e.g., breach event) on the treatment group (e.g., breached banks) while controlling for pre-treatment characteristics and common industry shocks. The pre-breach deposit, loan composition, operating expenditure, and industry shocks are assumed to impact the control group in terms of performance in the same way they would affect the treatment group. Then, the difference in the control group's performance can be used as the benchmark in the absence of a significant change in the breach event. Specifically, the difference between the estimate for the treatment group and the benchmark provides a causal effect of the breach on bank performance. We use the following difference-in-difference regression to examine the effects of cyber breaches on bank performance:

- $PERF_{it} = \alpha + \beta_1 BREACH_{it} + \beta_2 POST_{it} + \beta_3 BREACH_{it} \times POST_{it} + \sum_4^n \beta_n X_{it} + \gamma_{it} + \theta_{it} + \varepsilon_{it}$

$PERF_{it}$ is the performance of bank *i* at quarter *t*. We employ three alternative measures of bank performance including return on asset (ROA_{it}), return on equity (ROE_{it}), and net interest margin (INT_{it}). $BREACH_{it}$ is an indicator that takes the value 1 if bank i at quarter t experiences a cyberattack and zero if bank i at time t is a nontarget matching bank. $POST_{it}$ is an indicator that takes the value 1 for bank-quarter in the post-attack period (quarter zero through quarter +12) and 0 for the pre-attack quarter (e.g., quarters -1 through quarter -12). The interaction term between and $BREACH_{it}$ is our variable of interest. X_{it} is a vector of control variables including *LNASSET, DEPOSIT, LOAN, NONPERLOAN, OPEREXP,* and *LIQUIDITY*. γ_{it} are the dummy variables for year-quarter fixed effects. θ_{it} are the dummy variables for the county location fixed effects. ε_{it} is the error term. We calculate the heteroskedasticity consistent standard errors.

We conducted several diagnostic tests to determine the appropriateness of the utilized estimation technique for our main model. First, we perform multicollinearity diagnostic tests for the control variables. The highest variance inflation factor (VIF) value is 2.87, and the lowest is 1.06; the average VIF is 1.918. Thus, multicollinearity is not an issue in our model. We also perform the Im-Pesaran-Shin panel data unit-root test with individual intercepts and automatic selection of maximum lag length based on the Schwarz Information Criterion, the Newey-West automatic bandwidth selection, and the Bartlett Kernel. The results provide overwhelming evidence that all series are stationary. Later, we conducted the Wooldridge test for autocorrelation in the panel data. The test statistics of 2.484 provides no statistically significant evidence that first-order autocorrelation is present with each panel. It is possible that bank performance might be affected by certain common shocks in the economy. Therefore, we test for the potential systematic bank performance using Pesaran's test for the cross-sectional independence between the panels. Pesaran's test statistics are -1.317 and insignificant, suggesting that cross-sectional dependence is not an issue between the panels. Finally, we test for panel-level heteroskedasticity employing the Wiggins and Poi (2003) LR test. The Chi-squared test statistics, which are significant at the 1%

level, suggest the presence of heteroskedasticity. To address this issue, we adjust the standard errors for clustering effects among observations of the same bank. These diagnostic tests indicate that our data does not suffer from panel-level autocorrelation and cross-sectional dependence. The results of these diagnostic tests are not tabulated, but the table is available upon request.

Findings

Impacts of Data Breaches on Bank Performance

Table 2 reports the results from the estimations of equation (1) for the weighted sample. Panel A reports the results using the data in the (-4, +4) quarters surrounding the date the breach is made public. In Panels B and C, we use the data in the (-8, +8) and (-12, +12) quarters, respectively. The coefficient on the variable of our interest, $BREACH_{it} \times POST_{it}$, is negative but insignificant in all three models in Panel A. These results suggest that experiencing a data breach does not harm short-term bank performance. These findings seem to support *the traditional theory of the firm*, which predicts that breached banks may not suffer negative performance consequences because they exist to maintain profitability.

However, our key findings demonstrate that in the longer term, breached banks experience a significant decline in their performance. ROA, ROE, and INT had declined by 0.099%, 1.448%, and 0.133% in the (-8, +8) quarters and by 0.149%, 1.824%, and 0.23% in the (-12, +12) quarters. This indicates that banks' long-term performance two and three years after a breach differs significantly from overall bank long-term performance in the post-breach period. Kamiya et al. (2021), using a sample that included only public firms across eight industries, showed that being breached does not affect performance two and three years after the incident. Our sample includes only banks. Our findings suggest that while banks suffer adverse effects of a cyberattack, it appears as if the effect takes longer than one year to manifest itself. These results support the prediction of *the idiosyncratic viral loss theory* that a cyberattack is an unexpected adverse event that negatively impacts breached banks' profitability in the long term.

We also perform the propensity score matching procedure similar to prior studies to identify the non-breached matching banks that have a similar likelihood of being targeted but have not been breached. We repeat the same analyses as in Table 2 using the propensity score matched sample. Although these results are not tabulated for brevity, they are available upon request. These findings support our claims stated in *Hypothesis 1* and answer our first research question. By statistically proving that cyberattacks negatively affect bank performance, our paper is a call for action that invites bank executives to manage cyber risk more effectively to avoid these incidents. Our findings should also concern the Federal Reserve Bank because any threat to the profitability of commercial banks may jeopardize the stability of the entire economy.

Impacts of Data Breaches on Bank Performance by Subsamples

Table 3 reports the results for the subsamples based on the different types of breaches. We group the breach events into HACK - hacks by an outside party or infected by malware (in Panel A) and NON-HACK - all remaining breach events (in Panel B). The coefficient on $BREACH_{it} \times POST_{it}$ variable is insignificant among HACK while negative and significant among NON-HACK in the (-8, +8) and (-12, +12) quarters. These results show that non-hack incidents mainly drive the

negative impact of data breaches on bank profitability and support *Hypothesis 2a*. Our findings imply that HACK incidents might compromise the integrity of precious bank-specific details, which may explain why these incidents have more damaging effects on bank profitability.

Table 2. Impact of Cyberattacks on Bank Performance - Entropy Balancing

	Panel A - (-4, +4)			***Panel B - (-8, +8)***			***Panel C - (-12, +12)***		
Variable	**ROE $_t$**	**ROA $_t$**	**INT $_t$**	**ROE $_t$**	**ROA $_t$**	**INT $_t$**	**ROE $_t$**	**ROA $_t$**	**INT $_t$**
BREACH	1.395***	0.221***	0.216**	2.112***	0.298***	0.247***	1.962***	0.299***	0.294***
	(2.867)	(3.669)	(2.469)	(5.363)	(6.074)	(3.626)	(5.415)	(6.692)	(5.022)
POST	0.766***	0.088**	0.141***	0.615***	0.073**	0.177***	0.649***	0.092***	0.252***
	(2.774)	(2.367)	(4.444)	(2.799)	(2.454)	(7.039)	(3.303)	(3.461)	(10.667)
BREACH * POST	-0.898	-0.068	-0.046	-1.448***	-0.099*	-0.133**	-1.824***	-0.149***	-0.230***
	(-1.540)	(-0.920)	(-0.597)	(-3.180)	(-1.711)	(-2.314)	(-4.530)	(-2.948)	(-4.747)
LNASSET $_{t-1}$	0.105	-0.042**	-0.086***	0.110	-0.047***	-0.087***	0.226**	-0.041***	-0.088***
	(0.637)	(-2.253)	(-3.977)	(0.871)	(-3.165)	(-5.037)	(1.998)	(-3.071)	(-5.891)
DEPOSIT $_{t-1}$	-5.012***	-1.030***		-5.739***	-1.067***		-5.815***	-1.067***	
	(-3.872)	(-6.475)		(-5.681)	(-8.884)		(-5.912)	(-9.041)	
LOAN $_{t-1}$	1.755	0.304		4.475***	0.583**		4.939***	0.598***	
	(0.553)	(0.661)		(2.649)	(2.490)		(3.822)	(3.495)	
NONPERLOAN $_{t-1}$	-0.783***	-0.065***	0.005	-0.856***	-0.065***	0.002	-0.908***	-0.069***	0.005
	(-10.993)	(-7.629)	(0.757)	(-14.186)	(-9.856)	(0.337)	(-15.032)	(-10.930)	(1.175)
OPEREXP $_{t-1}$	-0.092***	-0.006***	-0.017***	-0.102***	-0.009***	-0.015***	-0.108***	-0.009***	-0.014***
	(-8.669)	(-3.814)	(-8.928)	(-11.340)	(-7.184)	(-10.819)	(-12.886)	(-8.717)	(-12.468)
LIQUIDITY $_{t-1}$	-4.161	-0.264	-4.150***	-1.112	0.082	-4.003***	-0.390	0.163	-3.870***
	(-1.224)	(-0.503)	(-15.964)	(-0.635)	(0.305)	(-20.730)	(-0.297)	(0.842)	(-25.025)
Constant	21.521***	2.881***	7.426***	19.445***	2.869***	7.274***	17.455***	2.792***	7.103***
	(4.581)	(4.836)	(21.140)	(6.876)	(7.788)	(18.806)	(7.657)	(9.565)	(21.258)
Observations	107,451	107,451	107,451	194,085	194,085	194,085	272,088	272,088	272,088
Adj. R-squared	0.396	0.445	0.656	0.389	0.430	0.646	0.390	0.422	0.644

Note. ROE = Return on Equity; ROA = Return on Asset, INT = Net Interest Margin.

Table 3. Impact of Cyberattacks on Bank Performance - By Breach Types

Panel A – HACK	***Panel A1 - (-4, +4)***			***Panel A2 - (-8, +8)***			***Panel A3 - (-12, +12)***		
Variable	**ROE $_t$**	**ROA $_t$**	**INT $_t$**	**ROE $_t$**	**ROA $_t$**	**INT $_t$**	**ROE $_t$**	**ROA $_t$**	**INT $_t$**
BREACH	3.816***	0.744***	0.501***	4.240***	0.758***	0.497***	4.120***	0.709***	0.598***
	(7.131)	(12.250)	(7.138)	(9.578)	(14.114)	(8.324)	(10.924)	(15.711)	(12.287)
POST	0.512	0.065*	0.025	0.282	0.038	0.078***	0.373	0.044*	0.117***
	(1.389)	(1.707)	(0.860)	(1.085)	(1.274)	(3.645)	(1.564)	(1.649)	(6.096)
BREACH * POST	-0.488	0.006	0.128	-0.738	0.030	0.038	-0.696	0.032	-0.079
	(-0.653)	(0.068)	(1.523)	(-1.340)	(0.435)	(0.609)	(-1.478)	(0.530)	(-1.535)
Observations	27,198	27,198	27,198	49,980	49,980	49,980	71,526	71,526	71,526
Adj. R-squared	0.624	0.719	0.719	0.594	0.685	0.724	0.572	0.664	0.729
Panel B – NON-HACK	***Panel B1 - (-4, +4)***			***Panel B2 - (-8, +8)***			***Panel B3 - (-12, +12)***		
BREACH	0.621	0.084	0.196*	1.289***	0.162***	0.221***	1.190***	0.169***	0.253***
	(1.101)	(1.234)	(1.852)	(2.761)	(2.835)	(2.691)	(2.728)	(3.177)	(3.573)
POST	0.769**	0.089*	0.202***	0.782***	0.103***	0.199***	0.895***	0.132***	0.304***
	(2.017)	(1.821)	(4.421)	(2.865)	(2.825)	(6.121)	(3.696)	(4.067)	(10.183)
BREACH * POST	-0.980	-0.092	-0.092	-1.647***	-0.134*	-0.180**	-2.149***	-0.195***	-0.266***
	(-1.402)	(-1.068)	(-0.956)	(-2.945)	(-1.951)	(-2.485)	(-4.262)	(-3.163)	(-4.342)
Observations	80,253	80,253	80,253	144,105	144,105	144,105	200,562	200,562	200,562
Adj. R-squared	0.383	0.431	0.670	0.377	0.409	0.657	0.380	0.396	0.655

Note. ROE = Return on Equity; ROA = Return on Asset, INT = Net Interest Margin.

Table 4 reports the results for the subsamples based on bank size. In the quarter preceding the date the breach is made public, we group the universe of banks into terciles based on their assets. 5% of the breach target firms belong to the lowest tercile; 9.17% belong to the mid tercile, and 85.83% belong to the highest tercile. We report the results for ROA in Panel A, ROE in Panel B, and INT

in Panel C. Table 4 portrays the same story as in the study by Kamiya et al. (2021), who show that larger firms experience declines in ROA following cyberattacks. Specifically, the results on the $BREACH_{it} \times POST_{it}$ variable suggest that the negative effect of the breach on target banks is significant only among the largest tercile banks and only in the (-12,+12) quarters. This finding contradicts *Hypothesis 3.* Although larger banks have more financial resources to improve their cybersecurity practices, they also have a larger number of employees who require training in cybersecurity and have more complex computer networks that make information security a challenging task. In contrast, smaller banks may be more effective in training employees and managing their less complex information security systems.

Table 4. Impact of Cyberattacks on Bank Performance - By Bank Size

Panel A - ROE$_t$		**(-4, +4)**			**(-8, +8)**			**(-12, +12)**	
Variable	**Smallest**	**Mid**	**Largest**	**Smallest**	**Mid**	**Largest**	**Smallest**	**Mid**	**Largest**
BREACH	-5.005**	24.859***	0.721	-4.427***	5.293	1.238***	-8.620***	4.231	1.112***
	(-2.011)	(3.184)	(1.486)	(-3.360)	(1.089)	(3.136)	(-4.844)	(1.121)	(2.981)
POST	2.053**	-0.290	0.311	0.525	0.146	-0.091	-0.357	0.671*	-0.051
	(2.310)	(-0.251)	(1.091)	(1.282)	(0.295)	(-0.418)	(-0.808)	(1.724)	(-0.263)
BREACH * POST	-0.761	0.563	-0.485	-0.132	0.578	-0.749	1.120*	-0.558	-1.192***
	(-0.778)	(0.494)	(-0.814)	(-0.248)	(0.489)	(-1.599)	(1.885)	(-0.538)	(-2.883)
Observations	5,638	10,442	91,371	10,680	19,590	163,815	15,708	27,376	229,004
Adj. R-squared	0.599	0.632	0.417	0.552	0.659	0.394	0.550	0.638	0.400
Panel B - ROA$_t$		**(-4, +4)**			**(-8, +8)**			**(-12, +12)**	
BREACH	-0.238	2.820***	0.133**	-0.052	0.720	0.184***	-0.841***	0.599	0.168***
	(-0.686)	(3.497)	(2.111)	(-0.261)	(1.394)	(3.601)	(-2.928)	(1.404)	(3.628)
POST	0.050	-0.023	0.043	-0.419***	-0.007	0.002	-0.558***	0.062*	0.005
	(0.383)	(-0.205)	(1.100)	(-4.331)	(-0.154)	(0.051)	(-5.620)	(1.683)	(0.176)
BREACH * POST	0.232	0.029	-0.016	0.709***	0.042	-0.039	0.899***	-0.082	-0.087*
	(1.241)	(0.272)	(-0.206)	(4.374)	(0.390)	(-0.653)	(5.774)	(-0.874)	(-1.684)
Observations	5,638	10,442	91,371	10,680	19,590	163,815	15,708	27,376	229,004
Adj. R-squared	0.577	0.711	0.484	0.542	0.712	0.462	0.510	0.714	0.460
Panel C - INT$_t$		**(-4, +4)**			**(-8, +8)**			**(-12, +12)**	
BREACH	-0.066	0.337	0.217**	-0.179	0.204	0.211***	-0.302	0.134	0.228***
	(-0.232)	(0.482)	(2.443)	(-0.726)	(0.479)	(3.068)	(-1.433)	(0.357)	(3.868)
POST	-0.304**	0.532***	0.132***	-0.061	0.339***	0.198***	0.046	0.398***	0.285***
	(-2.409)	(2.848)	(3.718)	(-0.810)	(3.726)	(6.624)	(0.795)	(5.386)	(10.117)
BREACH * POST	0.578**	-0.333	-0.044	0.234*	-0.541**	-0.120*	0.045	-0.791***	-0.203***
	(2.471)	(-1.614)	(-0.533)	(1.781)	(-2.478)	(-1.935)	(0.383)	(-3.979)	(-3.855)
Observations	5,638	10,442	91,371	10,680	19,590	163,815	15,708	27,376	229,004
Adj. R-squared	0.761	0.495	0.691	0.814	0.420	0.675	0.821	0.428	0.672

Note. ROE = Return on Equity; ROA = Return on Asset, INT = Net Interest Margin.

Table 5 reports the results for the private and the public bank subsamples. The results on the $BREACH_{it} \times POST_{it}$ variable suggest that the negative effect of the breach on target banks is significant for both private and public banks in the (-,+8) and (-12,+12) quarters. When we focus on ROE, the coefficient is -1.163 for public banks and -1.637 for private banks. Since ROE measures profitability from a shareholder wealth perspective, our finding implies that publicly traded banks may prioritize their shareholders' wealth after a cyberattack and suffer a smaller decrease in their ROE ratios. ROA gives us an understanding of a bank's profitability from an asset management perspective. Public banks experience a smaller decrease in their ROA ratios after a breach. When we focus on the INT, the coefficient is -0.225 for public banks and -0.439 for private banks, showing that private banks face more significant declines in their interest margins than public banks do. These three findings collectively support *Hypothesis 4a*.

Channels Through Which Data Breaches Impact Bank Performance

In this section, we explore the possible channels through which cyberattacks affect bank performance in two steps. First, we examine how cyberattacks affect the contributing factors to bank performance. The untabulated results from the difference-in-difference regressions of DEPOSIT, LOAN, and LIQUIDITY are available upon request. The coefficient on the $BREACH_{it} \times POST_{it}$ variable is negative and significant in the (-8, +8) and (-12, +12) quarters, suggesting a reduction in deposits in the breached banks upon a breach.

The coefficient is negative and significant only in the regressions of LOAN in the (-12, +12) quarters. The coefficient is positive and significant only in the regressions of LIQUIDITY in the (-12, +12) quarters. Since bank deposits, loans, and liquidity might be interconnected, it is essential to note that our regressions focusing on one of these three constructs control for the other two. When we run the difference-in-differences regression on the change in bank deposits, we control the changes in loans and liquidity to isolate the impact of a data breach only on bank deposits. Overall, the results show that all three constructs are potential channels through which a cyberattack may affect a breached bank's profitability.

Table 5. Impact of Cyberattacks on Bank Performance – Public vs. Private Banks

Panel A - ROE $_t$	**(-4, +4)**		**(-8, +8)**		**(-12, +12)**	
Variables	**Public**	**Private**	**Public**	**Private**	**Public**	**Private**
BREACH	-0.171	5.585***	0.551	5.438***	0.328	4.330***
	(-0.374)	(3.702)	(1.530)	(4.656)	(0.948)	(4.268)
POST	0.529**	0.010	0.161	-0.077	0.136	-0.185
	(2.298)	(0.021)	(0.865)	(-0.224)	(0.756)	(-0.583)
BREACH * POST	-0.566	-1.187	-0.930**	-1.559	-1.163***	-1.637*
	(-1.005)	(-0.928)	(-2.142)	(-1.461)	(-2.978)	(-1.774)
Observations	78,920	28,531	142,343	51,742	199,765	72,323
Adj. R-squared	0.463	0.468	0.437	0.475	0.428	0.476
Other control variables	Yes	Yes	Yes	Yes	Yes	Yes
Panel B - ROA $_t$	**(-4, +4)**		**(-8, +8)**		**(-12, +12)**	
BREACH	0.119**	0.361*	0.190***	0.323**	0.156***	0.299**
	(2.073)	(1.939)	(4.251)	(2.302)	(3.755)	(2.466)
POST	0.061**	0.046	0.001	0.038	-0.001	0.059
	(2.210)	(0.784)	(0.059)	(0.843)	(-0.025)	(1.401)
BREACH * POST	-0.040	-0.066	-0.041*	-0.109*	-0.071**	-0.130**
	(-0.572)	(-0.440)	(-1.757)	(-1.869)	(-2.473)	(-2.209)
Observations	78,920	28,531	142,343	51,742	199,765	72,323
Adj. R-squared	0.511	0.512	0.482	0.512	0.470	0.515
Other control variables	Yes	Yes	Yes	Yes	Yes	Yes
Panel C – INT $_t$	**(-4, +4)**		**(-8, +8)**		**(-12, +12)**	
BREACH	0.271***	-0.249	0.235***	-0.013	0.232***	-0.014
	(3.341)	(-0.862)	(3.730)	(-0.057)	(4.225)	(-0.076)
POST	0.206***	-0.058	0.248***	0.002	0.338***	0.058
	(6.266)	(-0.930)	(9.322)	(0.051)	(13.145)	(1.367)
BREACH * POST	-0.057	-0.102	-0.127**	-0.319**	-0.225***	-0.439***
	(-0.730)	(-0.537)	(-2.239)	(-2.097)	(-4.744)	(-3.328)
Observations	78,920	28,531	142,343	51,742	199,765	72,323
Adj. R-squared	0.724	0.515	0.708	0.481	0.703	0.474
Other control variables	Yes	Yes	Yes	Yes	Yes	Yes

Note. ROE = Return on Equity; ROA = Return on Asset, INT = Net Interest Margin.

We then tie the effect of cyberattacks on the contributing factors DEPOSIT, LOAN, and LIQUIDITY to the impact on ROE in Table 6. We calculate the changes in ROE as the difference in the average ROE between the (+1, +4) and (-4, -1), the (+1,+8) and (-8, -1), and the (+1, +12) and (-12, -1) periods. We calculate the changes in DEPOSIT, LOAN, ASSET, NONPERLOAN, OPEREXP, and LIQUIDITY similarly. We regress the changes in ROE on the changes in these

six variables and BREACH. The regressions are performed separately for the subsamples with higher vs. lower than the sample median values of changes in contributing factors. If the security breach reduces firm performance by reducing DEPOSIT and LOAN and increasing LIQUIDITY, then we should observe a significant and negative relation between BREACH and bank performance among the subsamples of banks with lower changes in DEPOSIT, LOAN, and higher changes in LIQUIDITY.

In Table 6, the coefficient on the *BREACH* variable for (-12,+12) quarters is -3.343 and significant at 1% for bank deposits that are lower than the sample median, -3.125, and significant at 10% for bank loans that are lower than the sample median, and -3.095 and significant at 10% for bank liquidity that is higher than the sample median. These findings suggest that declines in bank deposits and loans and increases in liquidity are three significant channels. Altogether, these findings support our claims in *Hypothesis 5*, *Hypothesis 6*, and *Hypothesis 7* and answer our third research question. We repeat the same procedure to examine the impact on the other two profitability variables, ROA, and INT. The untabulated results yield similar conclusions and are available upon request.

Table 6. The Channel Effects of DEPOSIT, LOAN and LIQUIDITY on ROE

Panel A - (-4, +4) quarters	**DEPOSITCHG** (+1, +4) -(-4, -1)		**LOANCHG** (+1, +4) -(-4, -1)		**LIQUIDITYCHG** (+1, +4) -(-4, -1)	
Variables	**Low**	**High**	**Low**	**High**	**Low**	**High**
BREACH	-0.987	-0.084	-1.759*	2.395**	0.344	1.071
	(-0.674)	(-0.089)	(-1.747)	(2.395)	(0.550)	(1.074)
DEPOSITCHG (+1, +4) -(-4, -1)	91.431***	-5.708	-14.717	19.800**	11.357	-2.100
	(3.388)	(-0.499)	(-1.567)	(2.397)	(1.633)	(-0.196)
LOANCHG (+1, +4) -(-4, -1)	-107.895***	21.982	-59.793***	85.419**	-18.406	-25.192
	(-4.484)	(0.783)	(-4.505)	(2.003)	(-0.827)	(-1.177)
ASSETCHG (+1, +4) -(-4, -1)	0.741	-7.624***	-7.214***	-2.056	-0.589	-4.121*
	(0.224)	(-3.263)	(-3.095)	(-0.839)	(-0.347)	(-1.854)
NONPERLOANCHG (+1, +4) -(-4, -1)	-0.788**	-1.354***	-1.579***	-0.653**	-0.685***	-1.268***
	(-2.308)	(-4.613)	(-5.168)	(-2.459)	(-2.658)	(-4.403)
OPEREXPCHG (+1, +4) -(-4, -1)	-0.324***	-0.224***	-0.151***	-0.307***	-0.328***	-0.177***
	(-7.422)	(-5.322)	(-4.193)	(-6.950)	(-8.597)	(-5.008)
LIQUIDITYCHG (+1, +4) -(-4, -1)	-144.338***	11.813	-53.530***	75.933*	-23.114	-44.043**
	(-4.755)	(0.459)	(-3.865)	(1.909)	(-1.016)	(-2.003)
Observations	5,917	6,172	6,198	5,891	5,803	6,286
Adj. R-squared	0.459	0.508	0.624	0.440	0.410	0.605
Panel B - (-8, +8) quarters	**DEPOSITCHG** (+1, +8) -(-8, -1)		**LOANCHG** (+1, +8) -(-8, -1)		**LIQUIDITYCHG** (+1, +8) -(-8, -1)	
Variables	**Low**	**High**	**Low**	**High**	**Low**	**High**
BREACH	-2.066	-1.726*	-2.162**	-0.568	-0.331	-1.571
	(-1.248)	(-1.732)	(-2.183)	(-0.861)	(-0.619)	(-1.625)
Observations	5,956	6,133	6,195	5,894	5,822	6,267
Adj. R-squared	0.674	0.567	0.751	0.497	0.520	0.717
Panel C - (-12, +12) quarters	**DEPOSITCHG** (+1, +12) -(-12, -1)		**LOANCHG** (+1, +12) -(-12, -1)		**LIQUIDITYCHG** (+1, +12) -(-12, -1)	
Variables	**Low**	**High**	**Low**	**High**	**Low**	**High**
BREACH	-3.343*	-1.548	-3.125***	-1.577**	-0.309	-3.095***
	(-1.862)	(-1.617)	(-3.232)	(-2.064)	(-0.375)	(-3.420)
Observations	6,004	6,085	6,171	5,918	5,858	6,231
Adj. R-squared	0.752	0.590	0.797	0.502	0.665	0.768

Discussions and Conclusions

Conclusions

We motivate our main research question by contrasting two theories. While *the theory of the firm* posits that firms exist to maximize their profits and make adjustments to achieve this goal, *the*

idiosyncratic viral loss theory suggests that unexpected events will occur, resulting in losses and perhaps insolvency. Our study provides empirical evidence supporting the latter, revealing how profitability ratios decline over the subsequent quarters following a breach, mainly driven by non-hack incidents. While breaches impact large and medium size banks negatively, small banks improve their profitability. We find that both ownership structures are associated with a decline in profitability but the negative impact on private banks is more severe. Importantly, our study makes a unique contribution by documenting that the decrease in profitability for breached banks stems from decreased deposits and loans, along with increased liquidity. This multifaceted analysis enhances our understanding of the economic consequences of breaches.

Theoretical Implications

The empirical evidence documented in our study makes valuable contributions to different lines of literature. Our study challenges the prevailing theory of the firm by revealing that data breaches serve as an example of idiosyncratic risk, leading to reduced bank profits. Our findings bolster support for the idiosyncratic viral loss theory, reflecting how unexpected data breaches can interrupt banks' performance. Our research also expands the literature on cybersecurity and contributes to the relatively limited literature on bank ownership structure. Finally, our study provides refreshing empirical evidence that complements the literature on bank profitability.

Practical Implications

Our findings have several practical implications for all stakeholders. Bank managers should acknowledge that their institutions are more vulnerable to cyberattacks and face harsh consequences. Bank managers should emphasize cybersecurity training to prevent breaches due to insiders, unintended disclosures, and lost or stolen documents or devices. Private bank managers should handle cyber risk more deliberately since breaches are more detrimental to their profitability. Breached banks should find ways to restore customer trust to prevent a significant decrease in deposits, exert effort to continue to lend, and refrain from increasing liquidity since both actions would negatively influence their post-breach performance. Bank managers must keep their expenses under control for the next three years to minimize the damage.

Our findings also have implications for other stakeholders. For example, large and private bank customers should be aware that these institutions will reduce their lending capacity following a breach. These customers should be ready to find alternative sources of debt financing. This applies to both individuals seeking personal loans and businesses looking for commercial loans. Customers might benefit from working with smaller banks since these financial institutions do not bear the negative consequences of breaches as much as their larger peers. These implications extend to industry leaders since the difficulty in finding external debt financing hinders industrial growth. The Federal Reserve Bank should assist breached commercial banks to prevent liquidity hoarding or lending freeze.

Limitations and Future Research

We plan to expand our study by employing alternative data sources to verify all cyber incidents within the same sample period, utilizing information from the PRC website. Although our data is limited to 2018, an update may confirm the applicability of our conclusions to more recent times.

We will investigate the factors that enable small banks to outperform larger ones after a cyberattack, despite facing similar limitations on financing. We will also incorporate how a virtual work environment could be utilized to improve the security of information systems (Karovic et al., 2021) in commercial banks. Finally, acknowledging the revolutionary role of artificial intelligence and how its interactions with business models impact firm value and competitive advantage (Turktarhan et al., 2022), we will assess artificial intelligence governance in commercial banks and its influence on cybersecurity and performance recovery after bank breaches.

References

Abadie, A., & Imbens, G. (2000). *Simple and bias-corrected matching estimators for average treatment effects* (Working Paper No. 283). National Bureau of Economic Research https://www.nber.org/system/files/working_papers/t0283/t0283.pdf

Austin, P. C. (2011). An introduction to propensity score methods for reducing the effects of confounding in observational studies. *Multivariate Behavioral Research*, *46*(3), 399–424.

Barry, T. A., Lepetit, L., & Tarazi, A. (2011). Ownership structure and risk in publicly held and privately owned banks. *Journal of Banking & Finance*, *35*(5), 1327-1340.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment* (Working Paper No. 18/143). International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

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), 69–104.

Chen, Y. K., Shen, C. H., Kao, L., & Yeh, C. Y. (2018). Bank liquidity risk and performance. *Review of Pacific Basin Financial Markets and Policies, 21*(1), 1-40.

Christaria, F., & Kurnia, R. (2016). The impact of financial ratios, operational efficiency and non-performing loan towards commercial bank profitability. *Accounting and Finance Review*, *1*(1), 43-50.

Duffie, D., & Younger, J. (2019). *Cyber runs* (Working Paper No. 51). Hutchins Center on Fiscal & Monetary Policy at Brookings. https://www.brookings.edu/wp-content/uploads/2019/06/WP51-Duffie-Younger-2.pdf

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2021). *Cyber risk and the U.S. financial system: A pre-mortem analysis* (Report No. 909). Federal Reserve Bank of New York. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf?sc_lang=en

Eling, M., & Zhu, J. (2018). Which insurers write cyber insurance? Evidence from the U.S. property and casualty industry. *Journal of Insurance Issues*, *41*(1), 22-56.

Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503–519.

Gogolin, F., Lim, I., & Vallascas, F. (2021). *Cyberattacks on small banks and the impact on local banking markets*. SSRN. http://dx.doi.org/10.2139/ssrn.3823296

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi 10.3233/JCS-2009-0398

Hainmueller, J. (2012). Entropy balancing for causal effects: A multivariate reweighting method to produce balanced samples in observational studies. *Political Analysis*, *20*(1), 25-46.

Iyer, S. R., Simkins, B. J., & Wang, H. (2020). Cyberattacks and impact on bond valuation. *Finance Research Letters*, *33*, 1-11.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305-360.

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

Karovic, V., Bartalos, J., Karovic, J., & Gregus, M. (2021). Enterprise environment modeling for penetration testing on the OpenStack virtualization platform. *Journal of Global Business Insights, 6*(14), 117-140.

Kashyap, A. K., & Stein, J. C. (2000). What do a million observations on banks say about the transmission of monetary policy? *The American Economic Review*, *90*(3), 407-428.

Kashyap, A.K, & Wetherilt, A. (2019). Some principles for regulating cyber risk. *AEA Papers and Proceedings, 109*, 482-487.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, *17*(2), 13-22.

Kwan, S. H. (2004). Risk and return of publicly held versus privately owned banks. *Economic Policy Review, 10*(2), 97-107.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *The Financial Review*, *53*(2), 413–455. https://doi: 10.1111/fire.12160

Mullineaux, D. (1978). Economies of scale and organizational efficiency in banking: A profit-function approach. *Journal of Finance*, *33*(1), 259-280.

Servidio, J. S., & Taylor, R. D. (2015). Safe and sound: Cybersecurity for community banks. *Journal of Taxation & Regulation of Financial Institutions*, *28*(4), 5-14.

Statista. (2023). *Spending on cybersecurity in the United States from 2010 to 2018*. https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

Turktarhan, G., Aleong, D. S., & Aleong, C. (2022) Re-architecting the firm for increased value: How business models are adapting to the new AI environment. *Journal of Global Business Insights, 7*(1), 33-49.

Velez, S. (2021). Idiosyncratic viral loss theory: Systematic operational losses in banks. *Journal of Risk and Financial Management*, *14*(2), 1-13.

Vernon, J. (1971). The separation of ownership and controlled and profit rates, the evidence from banking: Comment. *Journal of Financial and Quantitative Analysis*, *6*(1), 615-625.

Wiggins, V., & Poi, B. (2003) *Testing for panel-level heteroskedasticity and autocorrelation*. StataCorp FAQs. https://www.stata.com/support/faqs/statistics/panel-level-heteroskedasticity-and-autocorrelation/

Zakrzewski, A., Tang, T., Appell, G., Hardie, A., Hildebrandt, N., Kahlich, M., Mende, M., Muxi, M., & Xavier, A. (2019, June 20). *Global wealth 2019: Reigniting radical growth*. Boston Consulting Group. https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth