Cyberattacks on Small Banks

Fabian Gogolin
University of Leeds

Ivan Lim
Durham University

Francesco Vallascas*
Durham University

Preliminary and Incomplete

Abstract

Using a difference-in-differences design based on exogenous cyber incidents, we document that successful cyberattacks on small US banks reduce deposit growth at branches of affected banks. This result is more pronounced for the affected branches in counties where digital literacy is low or where the reputational advantage of competitors is high. Cyberattacks lead to a redistribution of deposits in favor of the dominant or largest (unaffected) banks in the local deposit market and generate negative consequences for the affected banks also in the mortgage market. Overall, our analysis shows that cyberattacks reduce the trust of bank customers by generating bank-specific reputational damages and highlight how costly financial constraints in cybersecurity investments can be for small banks.

JEL Classification: G21, G28.
Keywords: Small Banks, Cyber Risk, Depositors, Bank-specific information.

**Corresponding Author. Fabian Gogolin (F.Gogolin@leeds.ac.uk) is at Leeds University Business School, University of Leeds, 16 Clarendon Place, LS2 9JY. Francesco Vallascas (Francesco.Vallascas@durham.ac.uk) and Ivan Lim (Ivan.Lim@durham.ac.uk) are at Durham University Business School, Durham University, Mill Hill Lane, DH1 3LB.

1 Introduction

With the fast-growing technological content of banking products, cybersecurity represents a key and rising concern for regulators and bankers[1]. FDIC Chairman Jelena McWilliams stated that *"[c]ybersecurity is the biggest threat facing America's banks"*[2]. Indeed, the banking industry is seen as particularly vulnerable to cyber risks because of its high degree of interconnectedness, IT intensity and dependence on customer information as key inputs to the production process (Basel Committee on Banking Supervision, 2018; Duffie and Younger, 2019; Crisanto and Prenio, 2017; Eisenbach et al., 2020; Mester et al., 2019). Cyberattacks can lead to a loss of trust in stakeholders, and this loss might be especially detrimental in banking and challenge the sustainability of its business model (Chen et al., 2019; Kamiya et al., 2020).

Maintaining high cybersecurity protection of bank clients and minimizing the reputational damages that arise when cyber incidents occur have become key objectives for financial institutions (Kashyap and Wetherilt, 2019). According to a recent survey by Deloitte (2019) the average yearly investment by banks on cybersecurity has now surpassed 10% of the overall IT budget, equivalent to $2,300 per employee. In this landscape, small banks appear strongly disadvantaged. Although exposed to similar cyber risks as large banks, small banks find it more difficult to maintain this significant investment in human capital and technology required to protect their customers due to limited resources. Indeed, Nationwide reports that small banks with assets less than $1billion fall victims to almost half of cybercrimes between 2012-2017[3]. It is not surprising, therefore, that more than 70% of small bankers have recently

[1] See "US banks face tighter scrutiny of cyber defences", FT (2019), available at https://www.ft.com/content/69a25232-8eaa-11e9-a1c1-51bf8f989972; "Heightened Cybersecurity Risk Considerations", FDIC (2020).

[2] See "Banks could get fined for cyber breaches, top regulator says", CNN (2019), available at https://edition.cnn.com/2019/08/01/investing/fdic-cyber-hack-fine/index.html.

[3] See "5 Cybersecurity Myths Banks Should Stop Believing", Forbes (2019), available at https://www.forbes.com/sites/ronshevlin/2019/04/08/5-cybersecurity-myths-banks-should-stop-believing/#6c83bb1d630d.

ranked cybersecurity as their top concern (Conference of State Bank Supervisors, 2019).

Despite the pervasiveness of cybersecurity risks in the banking industry, however, there is no empirical assessment of how deficiencies in cybersecurity affect the business of small banks. This assessment is important to shed light on whether inadequate cybersecurity investments might reduce confidence on these banks and, consequently, hinder their key role in supporting the development of small businesses and the local economy. In fact, small banks have informational advantages in lending to small businesses which account for 99.7% of employee firms and almost half of private-sector employees (Stein, 2002; Liberti and Mian, 2008; Berger et al., 2005; Berger and Turk-Ariss, 2015; Agarwal and Hauswald, 2010; Hakenes et al., 2015; Skrastins and Vig, 2019). Furthermore, examining the implications of cyber risks on small banks is important to understand the benefits of adopting mechanisms, based on coordinated industry and regulatory initiatives that reduce financial constraints on these banks, to increase protection and mitigate losses in the case of cyberattacks that affect the trust of bank customers[4].

This paper offers the first empirical study of the consequences of cyberattacks on the market position of small banks. We base our analysis on exogenous data breaches involving small US banks covered in the Privacy Rights Clearinghouse (PRC) database over the period 2005-2017. We employ these exogenous events to implement difference-in-differences analyses that primarily assess how successful cyberattacks influence depositor behavior and, consequently, the competitive position of a small bank in the deposit market. Our focus on this market is motivated by two reasons. First, depositors can be significantly damaged by data breaches that compromise the confidentiality of personal information, potentially resulting in fraud, identity thief and subsequently, financial losses. Second, and more importantly, deposit markets are a key source of funding for small banks and their relationships

[4] See, for instance, "Countering Cyber Risk for Community Banks and Their Small Business Partners", Independent Community Bankers of America, available at https://www.icba.org/docs/default-source/icba/advocacy-documents/testimony/2015th-congress/testimony-3-8-17.pdf?sfvrsn=b73b6617_0.

with depositors are based on trust (Chen et al., 2019). Therefore, if cyberattacks damages the trust extended by depositors to small banks and leads to a weakening of banks' position in deposit markets, the long-term sustainability of the entire business model of these banks might be affected.

We start by documenting that the branches of small banks targeted by a data breach experience a significant slowdown in the growth rate of their deposits as compared to a control group of branches of banks of similar size. The effect of the cyberattack on deposits is also economically large. We find that a successful cyberattack reduces the average growth rate of deposits in the affected branches by more than 20 percentage points relative to the control group. Consequently, this leads to a decline in deposit market share. Our results are robust to a number of alternative empirical settings, including the adoption of the estimation approach of Bertrand et al. (2004) and the aggregation of the deposit data to the bank-county level.

Our result is consistent with a demand-side interpretation wherein depositors react to negative reputational shocks following data breaches on small banks that reduce depositors' confidence in affected banks. However, recent studies document that not all depositors react in the same way to negative information on bank financial and social performance (Chen et al., 2019, 2020). In particular, Duffie and Younger (2019) and Eisenbach et al. (2020) argue that the consequence of cyber risk can be framed in the context of bank runs. From this perspective, the negative effects for banks can be driven primarily by more informed depositors or, alternatively, by less informed depositors when 'panic' is a key driver of the reaction. In a series of tests, we find evidence in line with a stronger effect from depositors that are plausibly less knowledgeable about cyber risk. This result complements findings by Chen et al. (2019) and Chen et al. (2020) who show that more sophisticated depositors-presumably due to the ability to understand information- display stronger reaction to more technical disclosures such as bank earnings and regulatory ratings on community involvement. Our findings suggest that cyberattacks, which are more salient and directly impact depositors, are likely to incite larger responses from unsophisticated customers of the bank who might not be fully aware of the consequences and remediation processes following data breaches.

We next document that the response of depositors to cyberattack on small banks depends also on the market strength of its competitors. We show that the negative effects in terms of deposit growth for the branches belonging to affected small banks are larger in local deposit markets where competitors have a stronger leadership in terms of branch networks. We interpret this finding as indicating that negative reputational signals produced by cyberattacks on small banks are more pronounced when competitors have a strong reputational advantage (Dick, 2007).

Next, we test if negative reputational damages produced by a cyberattack might lead to negative consequences on small banks in terms of funding costs. Small banks might be forced to counterbalance the reputational loss produced by the cyber incident by offering a higher remuneration in their deposit products in order to maintain (or establish) contractual relationships with creditors. Accordingly, we examine whether the deposit rates offered by small banks to depositors change after cyberattacks. While we do not find a generalized increase in funding costs for branches of treated banks, we provide evidence of a response that differs across local deposit markets. We show that affected branches increase the offered rates only if located in markets where competitors do not have a strong advantage in their market leadership. Simultaneously, we observe a decrease in rates in markets where it is costlier to retain deposits because customers have more opportunities to switch to banks with a strong market leadership (Berger and Turk-Ariss, 2015; Jacewitz and Pogach, 2018). Essentially, our results indicate that, in response to cyberattacks, small banks modify the pricing policy of deposit products with the purpose of defending their market position in only some selected local markets to limit the overall increase in funding costs.

After examining the effects of cyberattacks on deposit growth rates and funding costs, we examine if cyberattacks generates spillover effects in local deposit markets. There are two contrasting views on the potential direction of these spillovers. A first view indicates that reputational damages can spread at the industry level and generate negative spillovers on unaffected banks. Using a sample of non-financial firms Kamiya et al. (2020) show negative value effects for firms operating in the same industry as those targeted by cyberattacks. Eisenbach et al. (2020) point out that in the case of financial institutions, cyberattacks can generate negative spillovers to other institutions via network effects (for instance, through the payment system). A second view suggests that the reputational consequences might remain bank specific and accordingly favor the reallocation of deposits towards other banks (Chen et al., 2019). We find evidence in support of this latter argument. We show that cyberattacks generate positive spillovers although only towards branches of non-affected dominant or large banks.

In a final group of tests, we analyze whether cyberattacks have negative reputational implications on the lending business of treated banks. Focusing on the mortgage segment of the lending market, and using the Home Mortgage Disclosure Act (HMDA) database, we conduct two sets of tests. The first takes the borrower perspective and examines the effects of cyber incidents in terms of the number and composition of mortgage applications that affected banks receive. The second focuses on the bank perspective and assesses the consequences of the incident on underwriting standards. We do not find that treated banks suffer from a decline in the number of mortgage applications after reputational shocks. Nevertheless, we document that the affected banks are more likely to attract riskier borrowers after the exogenous cyber incident and are forced to relax their lending standards to maintain mortgage approval rates.

Taken together, our findings document that cyberattacks undermine the trust of bank customers on the affected banks and generate significant bank-specific reputational damages but not negative spillovers on other (unaffected) institutions. These damages result in negative business effects in the deposit market for affected banks that take the form of a reduced competitive position. Reputational damages from cyberattacks also seem to partially affect treated banks in mortgage markets, not by a reduction in the nominal amount of loans received but by quality of loans that were received.

We contribute to three streams of research. The first consists of the growing literature on cyberattacks to corporations. To date this literature has primarily focused on non-financial firms and documented that the negative reputational effects produced by cyberattacks result in reduced shareholder value and risk appetite (Kamiya et al., 2020), decreased profitability (Akey et al., 2018), higher borrowing costs and tighter covenant intensity (Binfare, 2020) and higher audit fees (Li et al., 2020; Rosati et al., 2019). However, empirical investigations on the implications of cyberattacks on bank outcomes are almost non-existent. Eisenbach et al. (2020) simulate the potential externalities produced by cyberattacks through the wholesale payments network and show that damages to the five most active banks would affect more than a third of the network. Bouveret (2018) presents a cross-country overview of cyber risk in the financial industry and proposes a framework for its quantification. Aldasoro et al. (2020) examine the evolution of the losses due to cyber events in the context of a broader examination of the dynamics of operational risks in a cross-country setting. They document that although cyber losses represent only a fraction of total operational losses, they account for a significant portion of total operational value-at-risk.

Our analysis offers the first empirical investigation of the impact of data breaches on banks by taking the perspective of small bank customers and not the shareholder perspective typically adopted in studies on non-financial firms. The banking industry provides an appropriate laboratory to exploit this perspective as the banking business is built on trust and confidence in the deposit market that when undermined, might have long-term negative implications for a bank.

Second, our analysis relates to the literature on operational risks in banking. Earlier studies show that most of the operational losses at US financial institutions are produced by failures in internal control systems (Chernobai et al., 2011). Along these lines, and more recently, Chernobai et al. (2020) document that operational risks are more pronounced in complex banks. Barakat et al. (2019) highlight the reputational damages in terms of value effects arising from media announcements of operational risk events especially when the information on the event is opaque. Although frequently classified as part of operational risks, cyber risk shows key peculiarities related to the potential loss of confidentiality and availability of data or to damages to the integrity of data or systems (Eisenbach et al., 2020; Mester et al., 2019). These aspects are a potential concern for all stakeholders that engage in a contractual relationship with a bank and motivates our focus on deposit markets. Yet, contrary to existing studies on operational risks, we conduct our investigations only on events produced by external data breaches that are plausibly exogenous, allowing us to evaluate the causal implications of cyber risk on depositor behavior.

Finally, our analysis contributes to the literature on how depositors react to the disclosure of negative public information on banks. A first group of studies focuses on the disclosure of financial information by banks (Chen et al., 2020; Berger and Turk-Ariss, 2015; Iyer et al., 2016; Martinez Peria and Schmukler, 2001). The general consensus is that depositors react negatively in the presence of financial information highlighting negative bank performance, although there is heterogeneity in the response depending on the ability and incentives of depositors to monitor banks (Chen et al., 2020; Danisewicz et al., 2018). More closely related to our analysis are studies on how depositors respond to negative non-financial information. Chen et al. (2019) document that banks are more likely to suffer from larger deposit outflows when they show poor social performance measured through CRA ratings and CRA ratings downgrades. Homanen (2018) finds a similar negative effect in banks that financed the 2016 Dakota Access Pipeline project which crossed major rivers and ancient burial grounds.

None of these studies, however, focuses on non-financial events that can directly affect the contractual relationships between a bank and its depositors and documents how such events influence the re-distribution of deposits in a local market. The rest of the paper is structured as follows. Section 2 describes our empirical design with a particular focus on the sample and econometric setting. Section 3 presents the empirical results and Section 4 provides conclusions.

2 Identification Strategy and Data

2.1 Treated Banks and Econometric Model

We base our identification strategy on cyberattacks on small US commercial banks reported between 2005-2017[5]. We identify these attacks starting from the list of all data breach incidents involving financial institutions covered in the Privacy Rights Clearinghouse (PRC) database over the same period. The use of the PRC database is a conventional choice in the literature on cyberattacks and includes breaches that are reported in a timely manner under State Security Breach Notification Laws (Akey et al., 2018; Kamiya et al., 2020).

From the initial list of events involving financial firms, we retain in the sample only cyberattacks that satisfy three requirements: i) they are due to external data breaches (and not to bank employees) through which banks lost customer personal information by hacking or malware-electronic entry; ii) they target a small commercial bank (defined as a bank with total assets smaller than $10bln at the time of the data breach); iii) they affect banks for which we can identify detailed deposit data from the Summary of Deposits (SOD) provided by the FDIC. The first criterion ensures that the data breaches are plausibly exogenous and not caused by bank mismanagement. By applying these selection criteria, we identify 16

[5] We do not include more recent cyberattacks in our sample because the implementation of our identification strategy requires at least three years of bank data after the attack has been reported.

cyberattacks to small banks. Table 1 reports the list of these events and their description.

[TABLE 1 HERE]

The SOD offers information on deposits at the branch level and gives us the opportunity to implement a tight geographic matching between the branches of the small banks targeted by a cyberattack and branches in the control group. The tight geographic matching between the treated and the control group is important to limit confounding factors that make it difficult to control for if our focus is on a broader geographic region. For instance, Becker (2007) finds that cities with a higher fraction of seniors also have higher volumes of deposits. If seniors react differently to cyberattacks, and have different deposit trajectories, comparing branches from different regions might bias our results. More generally, by relying on data from the same, restricted geographic market for the two groups of branches, we reduce the potential impact of omitted factors that influence the supply and demand of deposits.

Specifically, we construct our econometric setting by identifying all branches of an affected small bank at the county level within the state where the cyberattack was reported. These branches represent our treated group. Next, for each county in a state where branches of a treated bank operate, we form a control group of branches that are owned by a commercial bank that has a similar size as the treated one. To ensure a high degree of similarity in size between the treated and untreated small banks, we proceed as follows. We divide the treated banks with assets below the \$10bln threshold in two size-based groups. The first group includes small banks with assets up to \$1bln and the second group includes treated banks with assets between \$1bln and up to \$10bln. When we match the branches of treated and control banks, the control group consists only of the branches of untreated banks falling into the same size group. Additional tests, reported in the Online Appendix, show that our results remain unchanged when we employ a tighter size matching.

Given the staggered nature of cyberattacks, similar to Gormley and Matsa (2011), we use a stacked difference-in-differences approach to estimate the causal impact of cyber risk on depositor behavior. We construct cohorts composed of treated branches for each cyber event and stack the events to estimate the average treatment effect. When constructing the next cohort, we include in the control group only branches of banks that have not previously experienced a cyberattack. This choice allows us to more cleanly capture the treatment effect (Gormley and Matsa, 2011; Guo et al., 2019). We estimate the average treatment effect using an estimation window of (-3;+3) years around each cyberattack for a total of 3,076 (12,384) observations belonging to branches of treated (untreated) banks. More formally, we estimate the following model:

$$\begin{aligned} \text{Ln(Deposits)}_{i,j,z,c,t} = {} & \alpha + \beta \text{Treated} \times \text{Post} + \textbf{BRANCH} \\ & + \textbf{COUNTY} \times \textbf{TIME} + \varepsilon_{i,j,z,c,t}, \end{aligned} \tag{1}$$

Where Ln(Deposits) is the logarithmic transformation of the amount of deposits in branch i of bank j in county z, and belonging to a cohort c at time t. **Treated** is a dummy that equals one if a branch belongs to a bank that has suffered from an exogenous cyberattack in the sample period and zero otherwise; **Post** is a dummy equal to one in the post-shock window (up to 3 years post the shock). The difference-in-differences estimate of the coefficient of **Treated** × **Post** is the difference between how the dependent variable changes in the branches of treated banks (namely, banks affected by the cyberattack) and in the branches of the untreated banks after the shock. Given that our dependent variable is measured as the logarithmic transformation of bank deposits in a branch, the estimated coefficient is approximately equivalent to the difference in the average growth rate of the US dollar value of deposits in the groups of branches of treated and untreated banks from the pre to the post shock period.

The model includes branch fixed effects (**BRANCH**) to control for any branch-specific differences. Furthermore, depending on the estimated specification, **COUNTY** × **TIME** is a vector of county × year fixed effects to account for time variant county factors that influence the deposit market. We estimate equation (1) with standard errors clustered at the bank-level to control for within bank correlation in the evolution of deposits across different branches. However, in the robustness section we document that our results remain unchanged if we cluster the standard errors at the commercial bank level.

[TABLE 2 HERE]

Initially, we do not include in equation (1) bank-specific control variables. This choice is motivated by the fact that any bank control is also likely to be affected by the cyberattack, making it difficult to draw any appropriate inference based on the coefficient of **Treated** × **Post** (Gormley and Matsa, 2011). Nevertheless, to mitigate concerns over omitted variables, we also report the results when we add to (1) a vector including a limited number of bank controls. This vector consists of the logarithmic transformation of bank total assets measured in thousands of US$ (**Size**), the ratio between net income and total assets (**ROA**), the tier 1 capital ratio (**Tier 1**), the fraction of non-performing loans to reflect credit risk (**NPL**), total loans divided by total assets (**Loan**) and the ratio between total assets and the number of employees (**Productivity**) that we employ as a proxy for bank productivity. Panel A of Table 2 show key summary statistics.

2.2 Comparing the Treated and Control Group and Testing for Parallel Trends

Our empirical strategy requires that the untreated group represents an adequate counterfactual. In this section, we present several stylized facts to confirm that our setting satisfies this requirement.

We start by showing that the branches, and the related commercial banks, in the treated and control groups are sufficiently similar in their characteristics before the cyberattack was reported. Columns (2) and (3) of Panel B of Table 2 show the average values of our dependent variable and bank controls for the treated and control group in the year before the event. Column (4) reports the normalized difference in bank characteristics between the two groups of banks (Brown and Earle, 2017; Nicoletti, 2018). The difference is defined as follows:

$$\text{NDIFF} = \frac{\bar{x}_i - \bar{x}_j}{\sqrt{s_i^2 + s_j^2}}, \tag{2}$$

Where $\bar{x}_i$ (s_i^2) is the mean (variance) of a variable for one of the untreated groups and $\bar{x}_j$ (s_j^2) is the mean (variance) of the same variable for the treated group. We note that the differences between the control group and the treated group are below the threshold value of 0.25. Imbens and Wooldridge (2009) highlight that a value below this threshold is necessary to ensure that the two groups of observations are sufficiently homogenous.

A further key assumption of a difference-in-differences setting is that in the absence of the cyberattack, treated and untreated branches would have shown a similar evolution in the amount of deposits. This assumption cannot be directly validated because we cannot observe the evolution of deposits in the treated group in the absence of the cyberattack. However, we follow a conventional approach in the literature to show that the parallel trend assumption is plausible. We examine if there are trend differentials between the treated and untreated groups before the exogenous event occurs. Essentially, if the two groups of banks follow similar trends in the value of deposits prior to the cyberattack, it is reasonable to conclude that the parallel trend assumption is not invalid.

To investigate pre-shock trend dynamics in the two groups we conduct three analyses. First, we follow Lemmon and Roberts (2010) and report in columns (1) and (2) of Panel C of Table 2 the average one-year change in the dependent variable across the two groups in the 3 years preceding the cyberattack. In column (3) we show the differences in the yearly change between the two groups of banks. For the parallel trend assumption to be plausible, these differences should not be statistically different from zero. Column (4) documents this is the case (according to a difference in means t-test).

Second, in Panel D we test for any pre-shock differential in trends in Ln(Deposits) using a regression model as in Chen et al. (2018) and Lin et al. (2020). We estimate our regression specification with Ln(Deposits) as the dependent variable and interact our treated dummy with yearly dummies (jtq) for the q lags/leads of the period around the cyberattack. The model includes branch and county × year fixed effects. A necessary condition for the parallel trend assumption to be plausible is that the two groups of branches do not show significant differences in the deposit dynamics in the years prior to the shock. Along these lines, we find that none of the coefficients on the interaction terms between the treated dummy and the year dummy variables before the cyberattack is statistically significant at conventional levels.

[FIGURE 1 HERE]

Finally, Figure 1 plots the estimated trend in Ln(Deposits) in the two groups of branches in the 3-year period before and after the cyberattack. We estimate the trends from a linear specification that accounts for fixed effects and bank controls. This Figure does not show clear differences in the trends followed by the two group of branches in the 3-year period preceding the cyberattack. The two trend lines seem instead to follow very different trends in the post-period where we observe a clear decline in the trend for treated branches as compared to the other branches.

3 Empirical Results

3.1 Deposits and Cyberattacks

This section shows how branch deposits of treated banks change in response to exogenous cyberattacks. We begin in Panel A of Table 3 with a simple univariate difference-in-differences analysis to estimate the average treatment effect. We compute the average differences in Ln(Deposits) between the post and the pre-event period for groups of treated and untreated branches and then test whether these differences significantly differ between the two groups using a t-test of mean equality. We find that, although both groups show a significant increase in Ln(Deposits) over the event window, the increase is significantly smaller for treated branches. This preliminary finding is consistent with a negative reputational effect in the deposit market arising from the cyberattack that results in a slowdown of deposit growth for affected small banks.

[TABLE 3 HERE]

In Panel B of Table 3, we extend the analysis of the estimation of the average treatment effect to a multivariate setting based on equation (1). As mentioned earlier, the key coefficient is the interaction term **Treated × Post** that measures the change in the dependent variable (Ln(Deposits)) in the treated group from the pre-shock period to the post-shock period as compared to the same change observed in the control group. We initially report the estimates from a model that only controls for branch and county× year fixed effects to avoid the bias arising from "bad" bank-specific controls. Next, in column (2) we control for bank size and in column (3) we add the remaining controls.

Throughout all specifications, and in line with the univariate analysis, the coefficient of **Treated × Post** is negative and statistically significant. This coefficient ranges from -0.216

in column (3) to -0.251 in column (1). Ultimately, the result consistently indicates that branches of banks affected by a cyberattack experience a decrease in the growth rate of their deposits as compared to the control group. The magnitude of the decrease in deposit growth is also economically large: using the model in column (3), we find that the treated branches report a deposit growth rate that is approximately 22 percentage points lower as compared to what we observe in the control group. Notably, none of the controls have a significant effect on the dependent variable.

A possible concern for our results is that the matching between treated and untreated banks does not fully remove the influence of unobserved bank heterogeneity due to size differentials. In the Online Appendix, we mitigate this concern by further refining our matching approach. Specifically, we divide the two size bins, banks up to $1bln and banks from $1bln to $10bln into quartiles. For instance, the first quartile of the first (second) size bin goes up to $250mln ($2.5bln). We then match banks in the treated group with untreated banks falling in the same quartile within each size category. As shown in the Online Appendix, this alternative matching approach reduces significantly the number of observations in our sample but leaves our key result largely unchanged.

In summary, the results above suggest that cyberattacks have significant funding implications for the affected branches that depend on depositors' behavior. While other studies on non-financial firms have shown the firm-level consequences of cyberattacks by taking the perspective of shareholders (Akey et al., 2018; Kamiya et al., 2020), we document how cyberattacks have implications on treated firms through the choices made by key stakeholders (namely, bank depositors).

3.2 Robustness Tests

3.2.1 Alternative Econometric Specifications

Table 4 reports additional specifications to show the robustness of our findings. First, Bertrand et al. (2004) argue that biased standard errors might arise from difference-in-differences analyses that focus on serially correlated outcomes. One of the remedies to mitigate this bias is to collapse the estimation period to one period before and one period after the shock. In the first, three columns of Panel A of Table 4 we show that our key result still holds under this alternative approach.

In the next three columns, we collapse the county-branch level observation to the bank-county level. This empirical design allows us to understand the overall effect of cyberattacks on deposit growth rates in local markets. We estimate several models at the bank-county level without and with bank controls. Each model includes bank fixed effects, county × year fixed effects and employs standard errors clustered at the bank level. In line with our branch-level analysis, we find that banks affected by cyberattacks show a relative decline in the growth rate of their deposits at the county-level as compared to banks in the control group.

Next in the first three columns of Panel B, we modify the baseline models by replacing county×year fixed effects with state×year fixed effects to account for the possibility that demand factors in the deposit market are influenced by state-level variables. Finally, in the last three columns of the same Panel, we re-estimate the initial branch-level models by clustering the standard errors at the branch (and not at the bank) level. All our findings remain largely unchanged when we employ these different empirical settings. Finally, in the Online Appendix, we follow Gormley and Matsa (2011) and replace branch fixed effects with branch × cohort fixed effects. Again, we find that our results remain largely unchanged.

[TABLE 4 HERE]

3.2.2 Falsification Test

In this section we further validate a causal interpretation of our results by implementing a falsification test. Specifically, we falsely assume that the cyberattacks happened four years before their actual date and then re-estimate the different model specifications reported in Table 2 by focusing on the 3 years before and the 3 years after the placebo date. By dating the events 4 years earlier than the actual date, we avoid any overlap between the post-estimation window in the placebo test and the pre-estimation window in our original empirical setting.

To conduct the test, we interact a dummy (**Treated Fake**) equal to one for the banks that have suffered from a cyberattack in our original setting with a dummy (**Post Fake**) taking a value of one in the three years after the false cyberattack. In any specification, the interaction term should not be significant to confirm the causal interpretation of our results. Consistent with this expectation, the analysis reported in the Online Appendix shows that the interaction term **Treated Fake** × **Post Fake** does not enter any specification with a significant coefficient. Therefore, the results of the falsification test support a causal interpretation based on the effects of exogenous cyberattacks on depositors' behavior.

3.2.3 Do Cyberattacks Reduce the Market Share of Affected Banks?

An alternative way to examine the effects of cyberattacks on the deposit market is to focus on the impairment of the market position of affected small banks as measured by market share. To quantify the effects on the market share of treated banks, we first aggregate the deposits data at the bank-county level and estimate difference-in-differences specifications where the dependent variable is the deposit market share of a bank j in a county z. We estimate the model using the sample of matched treated and untreated banks we have employed in our previous analyses. The estimated equation takes the following functional form:

$$\begin{aligned}\text{Market Share}_{i,z,t} = {} & \alpha + \beta \text{Treated} \times \text{Post} + \mathbf{BANK} \\ & + \mathbf{COUNTY} \times \mathbf{TIME} + \varepsilon_{i,z,t},\end{aligned} \tag{3}$$

Where the dependent variable is the market share of bank j, in county z at time t (that is, the deposits of bank j in county c divided by the total bank deposits in the same county), BANK is a vector of bank fixed effects and TIME is a vector of county *times* year fixed effects. We cluster the standard errors at the bank level.

[TABLE 5 HERE]

The results reported in Table 5 show that cyberattacks significantly reduces the market share of treated banks. The estimates indicate a decrease of approximately 1 percentage point of the market share of these banks as compared to the untreated group as a consequence of the cyber incident. This decline is also economically substantial given that the average county market share of a treated bank prior to cyberattacks is equal to 7.2%.

Overall, cyberattacks on small banks result in a significant slowdown of the growth rates of deposits leading to a consequent decline in their market share as compared to untreated banks of similar size.

3.3 Heterogeneity in Depositors' Response

3.3.1 Does Digital Literacy Matter for Depositors' Response?

In this section, we investigate if heterogeneity in depositor sophistication matters when reacting to cyberattacks in deposit markets. Ex-ante, it is not clear if sophisticated or informed depositors should react more to cyberattacks. On one hand, Chen et al. (2020) document that negative bank performance is primarily understood and penalized by more sophisticated depositors when banks are more transparent. Similarly, Chen et al. (2019) show that "sophisticated" depositors react more negatively to the disclosure of negative bank social performance (measured by Community Reinvestment Act (CRA) ratings and by their downgrade). Thus, following this line of work, we should expect a stronger response from sophisticated informed depositors as they are better able to understand the consequences of cyberattacks.

On the other hand, the implications of the results above might not hold for our analysis. Differently from Chen et al. (2019) and Chen et al. (2020), the disclosure event we examine does not directly raise concerns over bank (social) performance but instead more directly affects bank depositors through exposure of their personal information. Put another way, Chen et al. (2019)examine the release of technical information (the support a bank offers to the local community through loans to small businesses) while Chen et al. (2020)focuses on bank earnings. Both of these disclosures might be less directly related to depositors' welfare and might only be understood by a limited number of sophisticated depositors. This suggests that cyberattacks might elicit stronger response from unsophisticated depositors as they are more salient.

Furthermore, from a theoretical point of view, both Duffie and Younger (2019) and Eisenbach et al. (2020) suggest that the consequence of cyber risk for depositors can be framed within theories of bank run. As a result, what we observe is not necessarily the consequence of a response driven by the ability of depositors to adequately understand elaborate information on issues related to cybersecurity. Instead, the reaction of depositors to the disclosure of cyberattacks might also driven by uninformed (unsophisticated) depositors.

We try to disentangle the role of depositor awareness about cyber risk on our results by differentiating depositors on the basis of their degree of "digital literacy" that we measure using several socioeconomic characteristics of the local deposit market. Specifically, the first measure is based on estimates of the percentage of broadband subscriptions in a county provided by Tolbert and Mossberger (2020). The second is from Form 477 on internet access connections per thousands of households at the county level provided by the Federal Communication Commission and available at https://www.fcc.gov/general/broadband-deployment-data-fcc-form-477. We next identify treated counties with high (low) digital literacy and estimate the following specification (see Irani and Oesch (2016) for a similar approach):

$$\begin{aligned}\text{Ln(Deposits)}_{i,j,z,t} = {} & \alpha + \beta_1(\text{Treated High Digital Literacy} \times \text{Post}) \\ & + \beta_2(\text{Treated Low Digital Literacy} \times \text{Post}) \\ & + \mathbf{BRANCH} + \mathbf{COUNTY} \times \mathbf{TIME} + \varepsilon_{i,j,z,c,t},\end{aligned} \tag{4}$$

where β_1 (β_2) measures the differential impact of the shock for the group of branches located in counties with high (low) Digital Literacy, defined as counties with values of our two proxies below (above) the median in the group of treated counties. As in our baseline analyses, we estimate equation (4) without and with bank controls.

[TABLE 6 HERE]

The results reported of Table 6 show that the relative decline in deposits in the treated group is stronger in counties where depositors show (plausibly) a low digital literacy. In particular, we find that the coefficient of **Treated Low Digital Literacy** × **Post** is negative and significant across all specifications independently of which proxy of digital literacy we employ. The coefficient of **Treated High Digital Literacy** × **Post** is still negative but its magnitude is always statistically smaller than the coefficient of **Treated Low Digital Literacy** × **Post**.

We provide further support for the conclusion above by repeating the analysis with more indirect proxies of digital literacy. The first is the median household income in a county taken from the US Census bureau (with higher values denoting more digital literacy). The second is the per capita income form dividends, interests and rents with larger values indicating more depositor sophistication and consequently higher digital literacy. Using these alternative measures, we still find a stronger decrease in deposit growth in counties where depositors should have less digital literacy[6].

In general, our results indicate that the consequences of cyberattacks on the deposit market are not a reflection of the awareness of depositors to issues related to cyber risk. In contrast, they seem to reflect a broader and widespread reputational effect.

3.3.2 Does the Market Leadership of Competitors Matter?

In a deposit market where banks compete for deposits, the magnitude of the reputational damage produced by a successful cyberattack might be influenced by the reputation strength of the competing banks in the same market. To put it differently, in local markets where competitors have a strong leadership and visibility, thus representing an appealing alternative for depositors, we should observe a stronger negative effect in terms of deposit growth for affected banks if we are indeed capturing a reputation effect.

To understand if the conjecture above finds support in our data, we use SOD data to quantify the proportion of bank branches in the local deposit market owned by the top 3 banks operating in that market and not affected by a cyberattack. We then estimate equations similar to (4) by distinguishing affected branches operating in local deposit markets with strong and low market leadership by the competing banks. Essentially, we postulate that unaffected banks with a large proportion of the branch network in the local market have a reputational advantage as compared to other banks. This assumption is consistent with the approach adopted by previous studies to quantify the reputation of banks in the syndicate lending market (see, for instance, Ross (2010) and Bushman and Wittenberg-Moerman (2012)).

[TABLE 7 HERE]

[6] The results are available upon request.

We report the results of the test in Table 7. In line with our expectation, we find that the decline in the growth rates of deposits for the affected branches relative to the branches in the control group is driven by markets where competitors own a larger proportion of the branch network. In these markets the (relative) decline in the growth rate of the deposits of the affected banks is well above 30 percentage points.

3.4 Do Cyberattack Affect Funding Costs in the Deposit Market

The negative reputational damages for affected banks after a cyberattack might also generate consequences in terms of funding costs. For instance, banks with a weaker reputation in ensuring the cybersecurity of their depositors might be forced to offer a higher remuneration to maintain (or establish) contractual relationships with creditors. Therefore, in this section we analyze how deposit rates offered by banks to depositors change after cyberattacks. Our deposit rates data comes from RateWatch[7].

We focus on three types of deposit rates: 1) rates offered on all products (**All rates**); 2) 12-month Certificate of Deposits with an account size of $10,000 (**CD12mth10k**), and; 3) Money Market deposit accounts with an account size of $25,000 (**MM25k**). The initial focus on all rates allows us to understand if there is any change in total funding costs. The focus on the other two rates is important to understand the effects on the costs of the two most representative time and savings deposit products used by bank customers (Drechsler et al., 2017, 2018)[8]. This choice allows us to more cleanly observe changes, if any, on rates offered for a single homogenous product following cyberattacks.

To conduct our analysis, we estimate the following difference-in-differences model:

[7] RateWatch collects weekly branch level data since 2001 on rates offered for various products (e.g., Certificate of Deposits, Money Market Deposits, Savings Accounts, Interest Checking Accounts) of different nominal amounts and maturities and covers over 50% of bank branches in the U.S.

[8] Ben-David et al. (2017) notes that only a relatively small fraction of bank deposits is of a longer maturity than 12-months and therefore, these short-term deposits are more likely to reflect depositor sentiment.

$$\begin{aligned} \text{Rates}_{p,i,j,z,t} = \alpha + \beta \text{Treated} \times \text{Post} + \mathbf{BRANCH} \\ + \mathbf{COUNTY} \times \mathbf{TIME} + \varepsilon_{p,i,j,z,t,} \end{aligned} \tag{5}$$

Where p is the product belonging to branch i of bank j in county z, and belonging to a cohort c at time t (week). Rates is the logarithmic transformation of the rates offered and described earlier. As before, our key explanatory variable is **Treated** × **Post** and measures the change in deposit rates from the pre to the post shock period (defined as in equation (1)) in the group of treated banks as compared to the control group. However, differently from our baseline model in (5) we define Post as equals to zero (one) for the 36-months before (after) the month where the hack took place because we can observe deposit rates at high frequency intervals[9].

[TABLE 8 HERE]

We report the results in Panel A of Table 8. The first three columns show the results for the rates on all products (ln(All Rates)) while Columns (4)-(6) and (7)-(9) shows rates on ln(CD10mth10k) and ln(MM25k) respectively. Regardless of the deposit product and econometric specification, we find that treated branches do not increase rates in the deposit market as compared to control branches after a cyberattack. One possible explanation for this finding is that cyberattacks are costly due to expenses on remediating information technology systems and procedures (Kamiya et al., 2020). Furthermore, these costs could be disproportionately higher for small banks, thus resulting in limited resources being allocated to increase the remuneration to creditors to defend their market position.

[9] In particular, deposit rates are available at weekly intervals. However, we define Post using months instead of weeks because depositors might not have been made aware immediately and react in deposit markets. Other specifications are similar to equation 1).

However, the finding that the overall cost of deposits does not increase after cyberattacks does not exclude the possibility that treated branches increase their rates in at least some local deposit markets. Specifically, the previous section suggests that the negative impact of cyberattack on deposit growth is stronger (weaker) in markets where competitors hold a stronger (weaker) leadership position (presumably due to their established reputation). The possibility for the affected branches to retain deposits is therefore not equal across different local markets. To examine the implications of this result for the rate policy of the hacked banks, we modify the specification in Panel A by interacting **Treated High Competitor's Market Position × Post** and **Treated Low Competitor's Market Position× Post** defined in the previous section and display the results in Panel B of Table 8.

We find that the coefficient of the interaction **Treated High Competitor's Market Position × Post** (**Treated Low Competitor's Market Position× Post**) is negative (positive) and statistically different at conventional levels. Therefore, in counties where there is a strong (weak) market leadership position by competing banks, the treated branches decrease (increase) their rates offered on deposit products. This result indicates that treated banks increase the offered rates only in markets where they have plausibly more chances to compete with the unaffected banks; that is, when competing banks do not have a strong competitive advantage from their market leadership that makes it unlikely for the hacked banks to retain old (or attract new) customers. Simultaneously, the need to limit the overall costs paid on deposits seems to induce hacked banks to decrease deposit rates in markets where it is costlier to retain (or attract) bank customers; namely, in local markets where customers have the opportunity to switch to banks with an established and strong market position (Berger and Turk-Ariss, 2015; Jacewitz and Pogach, 2018).

Taken together, our analysis provides insight into how banks manage their funding strategy after losing trust in deposit markets brought upon by cyberattacks.

3.5 Spillover Effects in the Local Deposit Market

Our baseline analysis does not consider the possibility of spillover effects within a local deposit market. The assumption of a lack of spillover effects is rooted in any conventional difference-in-differences framework that excludes interferences across units by formally requiring that the Stable Unit Treatment Value Assumption (SUTVA) holds[10]. Nevertheless, in empirical settings involving companies operating in the same industry (and often in the same market), this assumption is less likely to be valid and the related estimation of the average treatment effect can be significantly biased (Boehmer et al., 2020; Clarke, 2017). For instance, Kamiya et al. (2020) show negative spillovers at the industry level after cyberattacks for non-financial firms and Eisenbach et al. (2020) point out that a cyberattack to one financial institution can generate negative spillovers on other institutions via a network effect (for instance, through the payment system). Therefore, given that banks compete in narrow geographic markets through branch networks, there could be concerns of spillover effects.

However, when cyberattacks involve small banks, it might well be possible that the events maintain an idiosyncratic nature. It follows, that under an "equilibrium framework" for the deposit market, at least part of the funding that are not deposited in the affected banks because of the cyberattack will remain still within the local deposit market (e.g., Chen et al. (2017)). As such, ex-ante, it is unclear if cyberattacks to small banks produces spillovers, and if so, its direction. In the next two sections, we model and test for two different typologies of spillovers: a) towards similar small banks; b) towards dominant or the largest banks in the local market.

[10] This assumption postulates that there are no indirect effects arising from treatment related to externalities. These externalities can influence the control group after the implementation of the treatment (Boehmer et al., 2020). The presence of potential geographic-related externalities is only one of the possible causes of indirect effects associated a treatment.

3.5.1 Spillover Effects Towards Small Banks

Spillovers towards small banks can occur for two reasons. First, negative spillovers might materialize if similar small banks are perceived equally at risk in terms of cybersecurity. Second, positive spillovers might emerge when depositors that conventionally opt for small banks still prefer to establish contractual relationships with banks of similar size. In both cases, these effects might affect our controls group, thus creating a potential bias in our estimates. In this section, we test for the presence of these spillover effects within our control group. To this end, we compare the dynamics of deposits in the branches of untreated banks in our control group in the counties where the hacked banks operate and with the dynamics of branches of banks with similar size operating in adjacent counties (where there are no hacked banks). We then estimate a difference-in-differences model where the original control group is considered (indirectly) "treated". As in our initial tests, we estimate the model with and without controls.

[TABLE 9 HERE]

We report the results in Panel A of Table 9. In all specifications, we do not find any evidence that the growth rate of the deposits of the branches of (indirectly) "treated" banks is significantly different from the growth rate of branches of similar banks in adjacent counties. In additional tests, we achieve a similar conclusion if we consider as (indirectly) "treated" banks, those institutions with assets up to $10bln and operating in counties where branches of hacked banks are located.

Two key conclusions emerge from the set of tests discussed above. First, it is unlikely that our initial estimates of the average treatment effects are biased due to the presence of small bank spillovers within the estimation sample. Second, and more generally, there is no evidence of any beneficial or damaging effects for similar banks from the cyberattack.

3.5.2 Spillover Effects towards Dominant and Large Banks

We next extend our analysis to account for the presence of potential spillovers in favor of dominant or large banks in the local market. Dick (2007)documents that service quality is higher in larger markets and especially for banks that dominate these markets. It might therefore be suggested that depositors would reallocate their deposit decisions towards these banks. To examine this, we exploit the dynamics of deposits in the branches of untreated large (or dominant) banks in the counties where affected small banks operate and in adjacent counties (where there are no affected small banks).

Specifically, in each of the affected county, we identify banks that have a dominant market position (market share larger than 20%) or that are large. We use three definitions of large bank: a) a bank with total assets above \$10bln; b) a bank with total assets above \$50bln and; c) a bank with total assets above \$100bln. We then compare the dynamics of the deposits of these banks with those of banks with a similar market position or size in adjacent counties unaffected by the cyberattacks around the events in our sample. We compare banks in adjacent counties as these banks are likely to be operating in similar observable and unobservable conditions that might influence the evolution of deposits (Huang, 2008). In essence, we estimate a difference-in-differences where we define as "treated" dominant (large) banks in the affected counties and as untreated the dominant (large) banks in the unaffected adjacent counties.

We report the results of these tests in Panels B, C, D and E of Table 9. More precisely, in Panel B we present the results for the sample of dominant banks while in remaining Panels we focus on banks with total assets above \$10bln (Panel C), \$50bln (Panel D) and \$100bln (Panel E).

The analysis consistently indicates an increase in the deposits for dominant and large banks operating in the counties affected by cyberattacks as compared to banks located in unaffected adjacent counties. The differential increase in deposit growth ranges between 7 and 8 percentage points. Taken together, we find strong evidence of positive spillovers effects towards dominant or large banks. This is consistent with the view that these banks might benefit from reputational advantages and are therefore able to capture the deposits that are lost from affected small banks.

3.6 Do Cyberattacks Affect a Bank's Reputation in the Local Lending Market?

Besides deposit markets, banks engage in contractual relationships with households in the lending market. While cyberattacks do not pose immediate threats to potential borrowers, they might still undermine a bank's reputation in the lending market and its competitive position (Akey et al., 2018; Kamiya et al., 2020). We examine the consequences of the cyberattacks in the lending market in two steps.

First, we take the perspective of the applicants to test whether potential borrowers shy away from banks that have suffered cyberattacks and whether the characteristics of these borrowers change. In particular, if cyberattacks lead to reputational damages in the lending market, less risky applicants that have more alternatives in mortgage markets might opt for lenders with a stronger reputation. We would then observe a decrease in the quality of the applicants to the affected banks.

Second, we analyze a bank's response to borrower behavior in terms of underwriting standards. To maintain their market position, these banks might be forced to approve riskier loans with a consequent deterioration of their lending standards.

To conduct our analysis, we use loan data from the Home Mortgage Disclosure Act (HMDA) database collected by the Federal Financial Institutions Examination Council (FFIEC)[11]. Each loan application in HMDA dataset contains information on borrower demo-

[11] HMDA is a loan-level dataset that covers all mortgage applications that have been reviewed by qualified financial institutions, both private and public. HMDA requires an institution to disclose any mortgage lending if it has at least one branch in any metropolitan statistical area and meets the minimum size

graphics (e.g., gender and race), loan characteristics (e.g., loan amount applied for, applicant income and type), the decision undertaken by the institution (e.g., approved or denied), the geographical location of the property (e.g., county), the year in which the loan application decision is made, and the lender's identifier.

It is worth noting that the HMDA data does not enable us to track the loans submitted to individual branches. Furthermore, because our primary interest is to observe the implications for the hacked banks and to reduce the effects of potential cofounding factors, we conduct the analysis at the bank-county-year level.

To construct our sample, we drop loan applications where the lender does not have a branch in the county of the mortgage's location. These observations are likely to be loans that were submitted to independent mortgage brokers (Cortés, 2015). Given that our initial tests focus on the response of potential borrowers of a bank that are geographically proximate to where the data breach occurred, retaining these observations is likely to introduce noise into the analysis. We then aggregate HMDA loan-level variables to the bank-county-year and estimate the following difference-in-differences model:

$$\begin{aligned}\text{Lending}_{i,z,t} = {} & \alpha + \beta \text{Treated} \times \text{Post} + \mathbf{BANK} \\ & + \mathbf{COUNTY} \times \mathbf{TIME} + \varepsilon_{i,z,t},\end{aligned} \tag{6}$$

Where Lending is one of the following variables includes 1) **Number of Loans** (the logarithmic transformation of the total number of loans submitted in a bank-county-year); 2) **Submitted Loan-to-Income Ratio** (the average loan amount requested for divided by the average income of the applicant in a bank county-year); 3) **Approval Rate** (number of approved loans/total loans submitted at the bank-county-year level); 4) **Approved Loan-to-Income Ratio** (the bank-county-year average of loan amount requested in approved

threshold. For instance, in 2010, this reporting threshold is \$39 million in book assets. The annual reporting criteria can be accessed at: https://www.ffiec.gov/hmda/reporterhistory.htm. Due to the low reporting requirements, the HMDA dataset covers the majority of lenders and accounts for nearly 90% of the U.S. mortgage market (Cortés et al., 2016).

loans/applicant income)[12]. The first two variables, therefore, take the borrowers' perspective while the remaining variables take the bank's perspective. We use Loan-to-Income ratios as a proxy for the riskiness of a borrower as higher values of these ratios indicate a lower capacity of borrowers to repay these loans, and as a result, lead to higher defaults on these loans (Dell'Ariccia et al., 2012; Campbell and Cocco, 2015).

Our key explanatory variable is **Treated** × **Post** and measures the change in one of the lending variables from the pre to the post shock period, defined as in equation 1), in the group of treated banks as compared to the control group. For all lending outcomes and specifications, we include a range of borrower and loan control variables.

[TABLE 10 HERE]

We report the results in Table 10. In the first two columns, we do not find evidence of an overall decline in the number of mortgage applications in the sample of the hacked banks as compared to the control group. However, the next two columns show a relative increase in the Loan-to-Income ratio of submitted loans in the group of hacked banks. The last four columns, taking the lender perspective, suggest that the approval rate of the affected banks does not change but there is an increase in the loan to income ratio of the approved loans. Taken together, these results indicate that treated banks are more likely to attract riskier borrowers after the exogenous cyber incident and are forced to relax their lending standards to maintain unchanged their approval rate.

Ultimately, the results are, at least partially, consistent with the reputational damages from data breaches in banking firms spilling over the mortgage market.

[12] We winsorize Applicant Income and Loan Amount at the 5% tails to minimize reporting errors.

4 Conclusion

Cybersecurity is a rising concern for regulators and bankers. However, while large banks have a wide range of human and financial resources to strengthen their defense against cyberattacks, small banks recognize cyber risks as the major threat to their business (Conference of State Bank Supervisors, 2019). In this paper, we document the validity of this view by identifying the negative business consequences for small banks after cyberattacks resulting in data breaches.

We show that the branches of small banks affected by exogenous cyber incidents experience a significant slowdown in the growth rate of their deposits as compared to branches of banks of similar size. This decline leads to a significant decrease in the deposit market share of the hacked banks. The negative effects of cyberattacks in local deposit markets are not driven by the awareness of depositors of the negative implications of cyber risk but seem to reflect a broader negative reputational effect. Along these lines, we show that the slowdown in deposit growth for hacked banks is stronger in local deposit markets wherein some competitors have a larger reputational advantage. Furthermore, while we do not find evidence of an aggregate increase in funding costs for the hacked banks after the cyberattack, we document these costs increase only in those local markets where these banks are more likely to defend their competitive position.

We next show that the cyberattacks generate positive spillovers on the branches of dominant and large banks in the local deposit market. Essentially, depositors opt for those banks that are normally associated with a better service quality in the deposit market (Dick, 2007).

Finally, we also find that the business damages for the banks targeted by a cyberattack extend also to the mortgage market. These banks attract riskier applicants after the cyberattack as compared to similar but untreated banks and are forced to relax their lending standards to maintain unchanged their approval rate.

Overall, our findings document that cyberattacks undermine the trust of bank customers on the affected banks and generate significant bank-specific reputational damages that lead to a reduced competitive position in the deposit market and to negative effects also for the contractual relationships of small banks with borrowers.

Therefore, the effects above implies that the presence of financial constraints on small banks in terms of cybersecurity investments has the potential to undermine the pivotal role of these banks for the development of local economies. In this respect, our analysis emphasizes the importance of sector cybersecurity initiatives which can complement the small bank-specific investments in cybersecurity strategies. Yet, equally important appears the implementation of cost recovery options that to reduce the negative reputational effects arising from data breaches.

Figure 1
Evolution of deposits over time

This figure plots the trend in Ln (Deposits) for branches of treated and untreated banks in the 3-year period before and after the cyberattack. We estimate the trends for a linear model that accounts for branch and county fixed effects and bank controls. This Figure does not show clear differences in the trends followed by the two group of branches in the 3-year period preceding the cyberattack. The two trend lines seem instead to follow very different trends in the post-period where we observe a clear decline in the growht rate for the branches of treated banks compared to the branches of untreated banks.

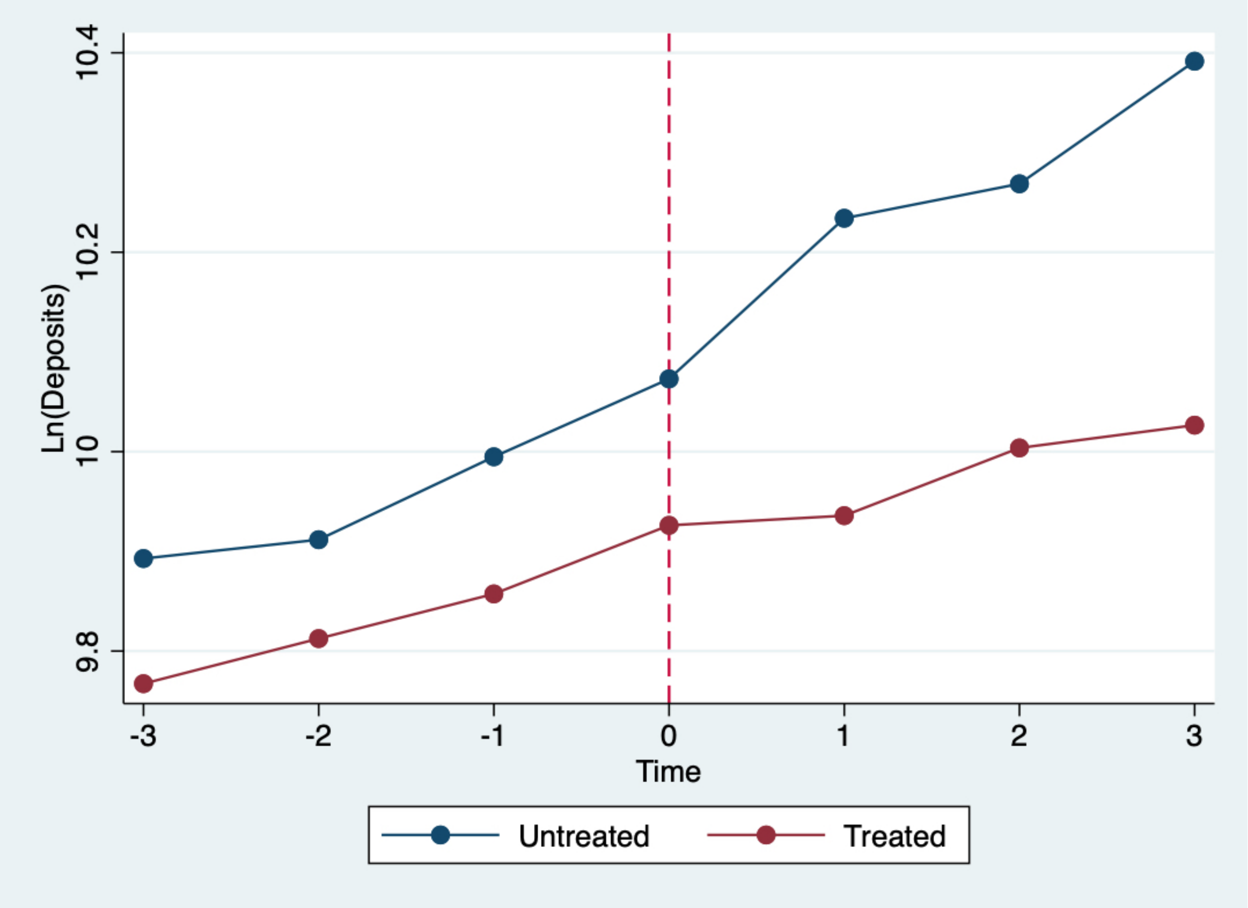

Table 1
Sample

The table below provides a description of the 16 cyberattacks considered in the analysis. We provide an overview of the report date, the bank identifier, the asset size in the year of the hack as well as geographic details including the state and the number of affected counties pertaining to the attack. In brackets is the number of all counties the bank operates in. The information on cyberattacks is provided by Privacy Rights Clearinghouse (PRC) the bank information is from the Summary of Deposits (SOD).

ID	Report Date	RSSDID	Assets (t-1)	Affected State	Affected Counties
1	May 19, 2006	682563	9595562	Texas	17
2	May 25, 2006	853372	313698	North Carolina	3
3	November 20, 2006	181758	52180	Louisiana	2
4	May 21, 2007	174572	3683951	New Jersey	10
5	October 10, 2007	500050	1293771	Kansas	4
6	January 24, 2008	975984	1021318	Texas	3
7	June 10, 2008	991340*	3509342	Indiana	8 (10)
8	August 28, 2008	816603*	2395586	Rhode Island	3 (4)
9	September 10, 2008	621076	321851	Ohio	1
10	January 12, 2010	799612	1569436	New York	1
11	November 16, 2010	616193*	124537	New Hampshire	1 (2)
12	January 31, 2013	997847	278904	Wisconsin	1
13	July 17, 2014	790534	2471993	Florida	1
14	January 4, 2016	618807*	3517028	Massachusetts	5 (4)
15	January 12, 2016	119779	745395	Massachusetts	1
16	January 12, 2016	128904*	8803622	Massachusetts	7 (11)

Table 2
Descriptive Statistics and Parallel Trends

The table below reports descriptive statistics and tests for parallel trends. Panel A provides descriptive statistics of the main variables used in the analysis. We use the natural logarithm of deposits (**Ln(Deposits)**) to estimate changes in deposits as a result of cyberattack. To control for bank-specific characteristics, we include a vector of control variables including the logarithmic transformation of bank total assets measured in thousands of US$ (**Size**), the ratio between net income and total assets (**ROA**), the fraction of non-performing loans to reflect credit risk (**NPL**), the tier 1 capital ratio (**Tier 1**), total loans divided by total assets (**Loan**) and a proxy for bank productivity defined by the ratio between total assets and the number of employees (**Productivity**). In Panel B, we compare the branches, and the related commercial banks, in the treated and control groups are sufficiently similar in their characteristics before the cyberattack. Columns (2) and (3) of Panel B of Table 2 show the average values of our dependent variable and bank controls for the treated group and the control group in the year before the event. Column (4) reports instead the normalized difference in bank characteristics between the two groups. In Panel C, we investigate pre-shock trend dynamics of our dependent variables across the two groups. We report the average one-year change in the dependent variable across the two groups in the 3 years preceding the cyberattack. In Panel D, we test for the presence of pre-shock differentials in our dependent variable using a regression model. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

Panel A: Descriptive Statistics

		Mean	Median	SD	Minimum	Maximum
Ln(Deposits)	15,460	10.080	10.601	2.316	0.000	13.472
Hack	15,460	0.199	0.000	0.399	0.000	1.000
Post	15,460	0.453	0.000	0.498	0.000	1.000
Size	15,334	14.821	14.905	0.969	11.379	16.398
ROA	14,730	0.010	0.009	0.008	-0.019	0.038
NPL	14,730	0.012	0.007	0.018	0.000	0.111
Tier 1	14,730	0.134	0.117	0.052	0.083	0.390
Loan	15,082	0.651	0.670	0.144	0.244	0.911
Productivity	15,080	5.348	4.783	2.930	0.673	16.325

Panel B: Pre-Shock Characteristics

	N	Treated (A)	Untreated (B)	Normalized Diff. (A-B)	Ttest (A-B)
Ln(Deposits)	2,328	10.095	10.038	-0.024	0.6436
Size	243	13.986	13.727	-0.129	0.4627
ROA	243	0.002	0.002	0.003	0.7818
NPL	243	0.014	0.016	0.109	0.6119
Tier 1	243	0.139	0.156	0.195	0.3867
Loan	242	0.661	0.674	0.069	0.7274
Productivity	231	4.823	5.641	0.248	0.2655

Panel C: Parallel Trends

	Treated (A)	Untreated (B)	Diff. (A-B)	T-value
Δ Ln(Deposits)$_{t-3}$	0.085	0.092	-0.007	0.826
Δ Ln(Deposits)$_{t-2}$	0.080	0.121	-0.041	0.190
Δ Ln(Deposits)$_{t-1}$	0.143	0.143	0.000	0.999

Panel D: Pre-Shock Trend Differentials

	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Dummy (t-3)	0.117	0.109	0.010
	(0.085)	(0.084)	(0.063)
Treated × Dummy (t-2)	0.115	0.107	0.100
	(0.079)	(0.076)	(0.072)
Treated × Dummy (t-1)	0.072	0.069	0.055
	(0.075)	(0.072)	(0.065)
Treated × Dummy (t+1)	-0.153***	-0.152***	-0.149***
	(0.049)	(0.049)	(0.052)
Treated × Dummy (t+2)	-0.151***	-0.148***	-0.141**
	(0.055)	(0.055)	(0.057)
Treated × Dummy (t+3)	-0.238***	-0.232***	-0.233***
	(0.058)	(0.058)	(0.057)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	15460	15334	14382
R^2	0.950	0.950	0.951

Table 3
Baseline Model

The table below reports difference-in-differences regression results where Ln(Deposits) is the logarithmic transformation of the branch-level deposits in US dollar. In Panel A we report a univariate difference-in-differences test. In Panel B we report our baseline regression. **Treated** is a dummy that equals one if a branch belongs to a bank that has suffered from an exogenous cyberattack in the sample period and zero otherwise; **Post** is a dummy equal to one in the post-shock window (up to 3 years post the shock). The difference-in-differences estimate of the coefficient of **Treated** × **Post** is the difference between how the dependent variable changes in the branches of treated banks (namely, banks affected by the cyberattack) and in the branches of the untreated banks after the shock. To mitigate concerns over omitted variables, we also report the results including a vector of bank controls. Depending on the specification, this vector consists of the logarithmic transformation of bank total assets measured in thousands of US$ (**Size**), the ratio between net income and total assets (**ROA**), the fraction of non-performing loans to reflect credit risk (**NPL**), the tier 1 capital ratio (**Tier 1**), total loans divided by total assets (**Loan**) and a proxy for bank productivity defined by the ratio between total assets and the number of employees (**Productivity**). Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Panel A: Univariate Ln(Deposits)		
	Treated	Untreated	Diff-in-diff
	(1)	(2)	(3)
Average Diff. Pre-Post	0.163**	0.371***	-0.209***
T-value	(3.734)	(18.140)	(4.490)
	Panel B: Multivariate Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	-0.250***	-0.241***	-0.216***
	(0.086)	(0.084)	(0.077)
Size		0.062	0.080
		(0.066)	(0.085)
ROA			3.547
			(3.547)
NPL			1.218
			(1.200)
Tier 1			-0.026
			(0.597)
Loan			-0.132
			(0.229)
Productivity			0.001
			(0.017)
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	15460	15334	14382
R^2	0.950	0.950	0.951

Table 4
Baseline Model: Alternative Specifications

The table below reports different specification to support the robustness of our difference-in-differences results. Panel A reports results for the model proposed by Bertrand et al. (2004) to control for potential autocorrelation in column (1) to (3) and county-bank level results in column (4) to column (6). In columns (4) to (6), we collapse branch-county deposits to the bank-county level and subsequently logarithmic transform bank-county deposits as we do in our main regression. Panel B reports results estimated using state fixed-effects in column (1) to (3) and results based on branch-level clustering in column (4) to (6). All regression include the appropriate controls consistent with our previous models. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level (branch-level) clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Panel A: Bertrand et al. (2004) Model and Bank-County					
	Ln(Deposits)					
	(1)	(2)	(3)	(4)	(5)	(6)
Treated × Post	-0.213***	-0.205***	-0.184**	-0.279***	-0.253***	-0.258***
	(0.077)	(0.075)	(0.077)	(0.084)	(0.086)	(0.076)
Size Control	No	Yes	Yes	No	Yes	Yes
Bank Controls	No	No	Yes	No	No	Yes
Branch FE	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	6594	6557	6303	2710	2679	2502
R^2	0.969	0.969	0.968	0.741	0.742	0.744
	Panel B: State FE and Branch Clustered SE					
	Ln(Deposits)					
	(1)	(2)	(3)	(4)	(5)	(6)
Treated × Post	-0.223**	-0.213**	-0.188**	-0.250***	-0.241***	-0.216***
	(0.090)	(0.087)	(0.077)	(0.086)	(0.084)	(0.077)
Size Control	No	Yes	Yes	No	Yes	Yes
Bank Controls	No	No	Yes	No	No	Yes
Branch FE	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	15460	15334	14382	15460	15334	14382
R^2	0.948	0.948	0.949	0.950	0.950	0.951

Table 5
Market Share

The table below reports results with respect to a bank's market share in the local deposit market. Therefore, we aggregate the deposits data at the bank-county level and estimate difference-in-differences specifications where the dependent variable is the deposit market share of a bank in a given county. Market share is constructed based on the market shares of banks obtained by scaling the dollar value of the deposits held by each bank in a county for the total amount of deposits in the same county. We estimate the model using the sample of matched treated and untreated banks we have employed in our previous analyses. The variable of interest is **Treated × Post**. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Market Share)		
	(1)	(2)	(3)
Treated × Post	-0.014***	-0.011***	-0.011***
	(0.002)	(0.002)	(0.002)
Size		0.011*	0.012
		(0.006)	(0.008)
ROA			0.119
			(0.135)
NPL			0.104*
			(0.054)
Tier 1			-0.007
			(0.044)
Loan			0.037*
			(0.021)
Productivity			0.002**
			(0.001)
Observations	2710	2679	2502
R^2	0.937	0.947	0.952

Table 6
Channel: Digital Literacy

The table below reports results concerning the heterogeneity in depositor responses to cyber attacks. We re-estimate our baseline regression and account for different dimensions of depositor digital literacy. In Panel A, we employ county measures related to the development of the infrastructure available in a county. The first indicator is based on the percentage of broadband subscriptions in a county provided by Tolbert and Mossberger (2020) and the results are reported in column (1) to (3). The second form is based on Form 477 on internet access connections per thousands of households at the county level and the results are reported in column (4) to (6). **Treated High Digital Literacy** × **Post** and **Treated Low Digital Literacy** × **Post** measure the differential impact of the shock for the group of branches located in counties with high (low) household sophistication, defined as counties with values of our two proxies below (above) the median in the group of treated counties. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

			Digital Literacy Ln(Deposits)			
	(1)	(2)	(3)	(4)	(5)	(6)
Treated High Digital Literacy × Post	-0.141**	-0.136**	-0.126*	-0.125**	-0.119**	-0.104**
	(0.067)	(0.067)	(0.069)	(0.055)	(0.055)	(0.051)
Treated Low Digital Literacy × Post	-0.434***	-0.427***	-0.384***	-0.424***	-0.416***	-0.384***
	(0.098)	(0.096)	(0.089)	(0.093)	(0.092)	(0.088)
Size Control	No	Yes	Yes	No	Yes	Yes
Bank Controls	No	No	Yes	No	No	Yes
Branch FE	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Coefficient	0.292***	0.292***	0.258**	0.299***	0.297***	0.280***
Observations	15460	15334	14382	15460	15334	14382
R^2	0.950	0.950	0.951	0.950	0.950	0.951

Table 7
Channel: Competitor's Market Position

The table below reports results concerning the heterogeneity in depositor responses to cyber attacks. We re-estimate our baseline regression and account for the largest three untreated banks in the local deposit market measured based on the market share of their branch network. We employ a measure based on the number of branches owned by a bank in a county scaled by the total number of bank branches in the same county (Benfratello et al., 2008). Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Competitor's Market Position Ln(Deposits)		
	(1)	(2)	(3)
Treated High Competitor's Market Position × Post	-0.392***	-0.381***	-0.342***
	(0.118)	(0.117)	(0.110)
Treated Low Competitor's Market Position × Post	-0.083	-0.078	-0.065
	(0.077)	(0.074)	(0.073)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Coefficient	-0.309***	-0.303***	-0.277**
Observations	15460	15334	14382

Table 8
Deposit Rates

The table below reports how deposit rates offered by banks to depositors change after cyberattacks. Our deposit rates data comes from RateWatch. Panel A reports results based on three types of deposit rates: 1) rates offered on all products (All rates); 2) 12-month Certificate of Deposits with an account size of $10,000 (CD12mth10k), and; 3) Money Market deposit accounts with an account size of $25,000 (MM25k). In contrast to our main analysis the **Post** period is defined as the 36-months before (after) the month where the hack took place. This choice is motivated by the higher frequency interval at which we can observe deposit rates data. Panel B reports results concerned with a heterogeneity in the effect on deposit rates. We re-estimate the regression in Panel A using the measure of market leadership position from Table 7. Again, we account for the largest three untreated banks in the local deposit market measured based on the market share of their branch network (Benfratello et al., 2008).

	All rates			CD 12MONTH 10k			MONEY MARKET 25k		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Treated × Post	0.019	0.012	0.015	-0.010	-0.005	0.000	0.022	0.043	0.046
	(0.021)	(0.022)	(0.023)	(0.017)	(0.024)	(0.027)	(0.049)	(0.059)	(0.061)
lSize Control	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Bank Controls	No	No	Yes	No	No	Yes	No	No	Yes
Branch FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3693464	3680156	3679981	23245	22988	22988	23652	23430	23430
R^2	0.389	0.382	0.382	0.977	0.977	0.978	0.967	0.966	0.966

Panel B: C3 (Branch)

	All rates			CD 12MONTH 10k			MONEY MARKET 25k		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Treated High Competitor's Market Position × Post	-0.013**	-0.014**	-0.013**	-0.027*	-0.027*	-0.025*	-0.043**	-0.043**	-0.043**
	(0.006)	(0.006)	(0.005)	(0.014)	(0.014)	(0.013)	(0.019)	(0.019)	(0.018)
Treated Low Competitor's Market Position × Post	0.071***	0.070***	0.077***	0.003	0.082***	0.103***	0.065	0.153***	0.159***
	(0.010)	(0.006)	(0.006)	(0.025)	(0.015)	(0.016)	(0.066)	(0.017)	(0.017)
Size Control	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Bank Controls	No	No	Yes	No	No	Yes	No	No	Yes
Branch FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Coefficients	-0.084***	-0.084***	-0.090***	-0.030	-0.109***	-0.128***	-0.108*	-0.197***	-0.202***
Observations	3693464	3680156	3679981	23245	22988	22988	23652	23430	23430
R^2	0.389	0.382	0.382	0.977	0.977	0.978	0.967	0.966	0.967

Table 9
Spillover Tests

The table below reports spillover tests. Panel A reports results of a spillover test to small banks. The spillover tests are constructed based on the size breakpoints we use in our main analysis. Small banks are defined as those untreated banks below 1bln and below 10bln respectively. Panel B reports results spillover tests to dominant banks. Dominant banks are defined as those that have a market share greater than 20% in the deposit market. Panel C, Panel D and Panel E report spillover tests to large banks defined as banks that have assets greater than 10bln, 50bln and 100bln respectively. **Treated** defined as all untreated banks in treated counties based on different size classifications. The tests are structured to compare untreated branches in treated counties with untreated branches in counties that are adjacent to the treated counties. All regression include the appropriate controls consistent with our previous models. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Panel A: Small Bank Spillover		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	0.023	0.029	-0.003
	(0.085)	(0.085)	(0.081)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	20826	20632	19236
R^2	0.947	0.949	0.953

	Panel B: Dominant Bank Spillover		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	0.073**	0.073**	0.072**
	(0.034)	(0.034)	(0.035)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	20459	20459	19691
R^2	0.926	0.926	0.927

	Panel C: Large Bank Spillover (>10bln)		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	0.072**	0.071**	0.083**
	(0.030)	(0.030)	(0.038)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	40382	40333	37203
R^2	0.900	0.900	0.906

	Panel D: Large Bank Spillover (>50bln)		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	0.066**	0.067**	0.084**
	(0.031)	(0.031)	(0.038)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	31378	31378	29788
R^2	0.899	0.900	0.904

	Panel E: Large Bank Spillover (>100bln)		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	0.076**	0.081**	0.101**
	(0.034)	(0.035)	(0.041)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	26023	26023	24573
R^2	0.902	0.903	0.908

Table 10
Mortgage Lending

The table below reports results of in respect to a bank's lending behavior. The loan data that comes from the Home Mortgage Disclosure Act (HMDA) database collected by the Federal Financial Institutions Examination Council (FFIEC). Lending is one of the following variables: 1) **Number of Loans** (the logarithmic transformation of the total number of loans submitted in a bank-county-year); 2) **Submitted Loan-to-Income Ratio** (the average loan amount requested for divided by the average income of the applicant in a bank county-year); 3) **Approval Rate** (number of approved loans/total loans submitted at the bank-county-year level); 4) **Approved Loan-to-Income Ratio** (the bank-county-year average of loan amount requested in approved loans/applicant income). Applicant income and loan amount are winsorized at the 5% tails to minimize reporting errors. For all lending outcomes and specifications, we include a range of borrower and loan control variables. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

			Mortgage Lending					
	Log(Number of Loans)		LTI		Approval rate		LTI Approved	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Treated × Post	0.103	0.106	0.166**	0.167**	-0.019	-0.020	0.111**	0.111*
	(0.148)	(0.148)	(0.073)	(0.073)	(0.021)	(0.023)	(0.055)	(0.057)
Log(NumLoans)			-0.636***	-0.638***	-0.033	-0.035	-0.747***	-0.747***
			(0.105)	(0.105)	(0.023)	(0.023)	(0.056)	(0.057)
Log(Total Loan Applied)			0.591***	0.593***	0.036	0.037	0.703***	0.703***
			(0.104)	(0.104)	(0.023)	(0.023)	(0.051)	(0.052)
Avg. Approvalrate							0.132	0.130
							(0.094)	(0.093)
Size Control	No	Yes	Yes					
Bank Controls	No	No	Yes					
Bank FE	Yes	Yes	Yes	Yes	Yes	Yes		
County x Year FE	Yes	Yes	Yes	Yes	Yes	Yes		
Observations	2033	2033	2033	2033	2033	2033	1992	1992
R^2	0.817	0.818	0.882	0.883	0.744	0.745	0.872	0.873

Online Appendix

Table A1
Robustness: Tighter Size Matching

The table below reports results on a tighter size matching of our control group of untreated banks. For the purpose of this test, the 2 size groups: 1) banks with assets up to $1bln and; 2) banks with assets from $1bln to $10bln are divided into quartiles. Following, we re-match our group of treated banks to control banks using this tighter size category and re-estimate our baseline regression. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Tighter Size Matching Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	-0.327***	-0.302***	-0.274***
	(0.097)	(0.090)	(0.087)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	4152	4149	3989
R^2	0.965	0.965	0.965

Table A2
Robustness: Alternative Fixed Effects and Falsification Test

The table below reports additional robustness tests for our main analysis. In Panel A, we specifically account for the fact that a number of events fall into the same cohort. In this alternative specification we include branch × cohort fixed effects. Panel B reports a falsification tests. We falsely assume that the cyberattacks happened 4 years before their actual date and then re-estimate the different model specifications reported in Table 2 by focusing on the 3 years before and the 3 years after the new date. By dating the events 4 years earlier than the actual date, we avoid any overlap between the post-estimation window in the placebo test and the pre-estimation window in our original empirical setting. To conduct the test, we interact a dummy (**Treated Fake**) equal to one for the banks that have suffered from a cyberattack in our original setting with a dummy (**Post Fake**) taking a value of one in the three years after the false cyberattack. Standard errors given in parentheses are corrected for heteroskedasticity and bank-level clustering. ***, **, and * indicate statistical significance at the 1%, 5% and 10% levels.

	Panel A: Cohort Fixed-Effects		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated × Post	-0.248***	-0.237***	-0.211***
	(0.086)	(0.083)	(0.076)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch x Cohort FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	15460	15334	14382
R^2	0.950	0.950	0.951

	Panel B: Falsification		
	Ln(Deposits)		
	(1)	(2)	(3)
Treated Fake × Post Fake	-0.445	-0.254	-0.047
	(0.327)	(0.199)	(0.045)
Size Control	No	Yes	Yes
Bank Controls	No	No	Yes
Branch FE	Yes	Yes	Yes
County x Year FE	Yes	Yes	Yes
Observations	13903	11064	7887
R^2	0.924	0.939	0.966

References

Agarwal, S. and R. Hauswald (2010). Distance and private information in lending. *The Review of Financial Studies 23*(7), 2757–2788.

Akey, P., S. Lewellen, and I. Liskovich (2018). Hacking corporate reputations. *Working Paper, Rotman School of Management*.

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach (2020). Operational and cyber risks in the financial sector. *Working Paper, BIS*.

Barakat, A., S. Ashby, P. Fenn, and C. Bryce (2019). Operational risk and reputation in financial institutions: Does media tone make a difference? *Journal of Banking & Finance 98*, 1–24.

Basel Committee on Banking Supervision (2018). Cyber-resilience: Range of practices.

Becker, B. (2007). Geographical segmentation of US capital markets. *Journal of Financial Economics 85*(1), 151–178.

Ben-David, I., A. Palvia, and C. Spatt (2017). Banks' internal capital markets and deposit rates. *Journal of Financial and Quantitative Analysis 52*(5), 1797–1826.

Berger, A. N., N. H. Miller, M. A. Petersen, R. G. Rajan, and J. C. Stein (2005). Does function follow organizational form? Evidence from the lending practices of large and small banks. *Journal of Financial Economics 76*(2), 237–269.

Berger, A. N. and R. Turk-Ariss (2015). Do depositors discipline banks and did government actions during the recent crisis reduce this discipline? An international perspective. *Journal of Financial Services Research 48*(2), 103–126.

Bertrand, M., E. Duflo, and S. Mullainathan (2004). How much should we trust differences-in-differences estimates? *The Quarterly Journal of Economics 119*(1), 249–275.

Binfare, M. (2020). The real effects of operational risk: Evidence from data breaches. *Working Paper*.

Boehmer, E., C. M. Jones, and X. Zhang (2020). Potential pilot problems: Treatment spillovers in financial regulatory experiments. *Journal of Financial Economics 135*(1), 68–87.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. *Working Paper, IMF*.

Brown, J. D. and J. S. Earle (2017). Finance and growth at the firm level: Evidence from sba loans. *The Journal of Finance 72*(3), 1039–1080.

Bushman, R. M. and R. Wittenberg-Moerman (2012). The role of bank reputation in "certifying" future performance implications of borrowers' accounting numbers. *Journal of Accounting Research 50*(4), 883–930.

Campbell, J. Y. and J. F. Cocco (2015). A model of mortgage default. *The Journal of Finance 70*(4), 1495–1554.

Chen, B. S., S. G. Hanson, and J. C. Stein (2017). The decline of big-bank lending to small business: Dynamic impacts on local credit and labor markets. *Working Paper, NBER*.

Chen, P.-Y., Y. Hong, and Y. Liu (2018). The value of multidimensional rating systems: Evidence from a natural experiment and randomized experiments. *Management Science 64*(10), 4629–4647.

Chen, Q., I. Goldstein, Z. Huang, and R. Vashishtha (2020). Bank transparency and deposit flows. *Working Paper*.

Chen, Y.-C., M. Hung, and L. L. Wang (2019). Depositors' responses to public nonfinancial disclosure. *Working Paper*.

Chernobai, A., P. Jorion, and F. Yu (2011). The determinants of operational risk in us financial institutions. *Journal of Financial and Quantitative Analysis 46*(6), 1683–1725.

Chernobai, A., A. Ozdagli, and J. Wang (2020). Business complexity and risk management: Evidence from operational risk events in us bank holding companies. *Journal of Monetary Economics*.

Clarke, D. (2017). Estimating difference-in-differences in the presence of spillovers. *Working Paper*.

Conference of State Bank Supervisors (2019). Community banking in the 21st century.

Cortés, K., R. Duchin, and D. Sosyura (2016). Clouded judgment: The role of sentiment in credit origination. *Journal of Financial Economics 121*(2), 392–413.

Cortés, K. R. (2015). Did local lenders forecast the bust? Evidence from the real estate market. *Working Paper*.

Crisanto, J. C. and J. Prenio (2017). Regulatory approaches to enhance banks' cybersecurity frameworks. *Financial Stability Institutions (FSI) Insights on policy implementation* (2).

Danisewicz, P., D. McGowan, E. Onali, and K. Schaeck (2018). Debt priority structure, market discipline, and bank conduct. *The Review of Financial Studies 31*(11), 4493–4555.

Dell'Ariccia, G., D. Igan, and L. U. Laeven (2012). Credit booms and lending standards: Evidence from the subprime mortgage market. *Journal of Money, Credit and Banking 44*(2-3), 367–384.

Deloitte (2019). Pursuing cybersecurity maturity at financial institutions. Technical report.

Dick, A. A. (2007). Market size, service quality, and competition in banking. *Journal of Money, Credit and Banking 39*(1), 49–81.

Drechsler, I., A. Savov, and P. Schnabl (2017). The deposits channel of monetary policy. *The Quarterly Journal of Economics 132*(4), 1819–1876.

Drechsler, I., A. Savov, and P. Schnabl (2018). Banking on deposits: Maturity transformation without interest rate risk. Technical report, National Bureau of Economic Research.

Duffie, D. and J. Younger (2019). *Cyber runs.* Brookings.

Eisenbach, T. M., A. Kovner, and M. J. Lee (2020). Cyber risk and the us financial system: A pre-mortem analysis. *Federal Reserve Bank of New York, Staff Report, 909*.

Gormley, T. A. and D. A. Matsa (2011). Growing out of trouble? corporate responses to liability risk. *The Review of Financial Studies 24*(8), 2781–2821.

Guo, B., D. Pérez-Castrillo, and A. Toldrà-Simats (2019). Firms' innovation strategy under the shadow of analyst coverage. *Journal of Financial Economics 131*(2), 456–483.

Hakenes, H., I. Hasan, P. Molyneux, and R. Xie (2015). Small banks and local economic development. *Review of Finance 19*(2), 653–683.

Homanen, M. (2018). Depositors disciplining banks: The impact of scandals. *Chicago Booth Research Paper* (28).

Huang, R. R. (2008). Evaluating the real effect of bank branching deregulation: Comparing contiguous counties across us state borders. *Journal of Financial Economics 87*(3), 678–705.

Imbens, G. W. and J. M. Wooldridge (2009). Recent developments in the econometrics of program evaluation. *Journal of Economic Literature 47*(1), 5–86.

Irani, R. M. and D. Oesch (2016). Analyst coverage and real earnings management: Quasi-experimental evidence. *Journal of Financial and Quantitative Analysis 51*(2), 589–627.

Iyer, R., M. Puri, and N. Ryan (2016). A tale of two runs: Depositor responses to bank solvency risk. *The Journal of Finance 71*(6), 2687–2726.

Jacewitz, S. and J. Pogach (2018). Deposit rate advantages at the largest banks. *Journal of Financial Services Research 53*(1), 1–35.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, forthcoming*.

Kashyap, A. K. and A. Wetherilt (2019). Some principles for regulating cyber risk. In *AEA Papers and Proceedings*, Volume 109, pp. 482–87.

Lemmon, M. and M. R. Roberts (2010). The response of corporate financing and investment to changes in the supply of credit. *Journal of Financial and Quantitative Analysis 45*(3), 555–587.

Li, H., W. G. No, and J. E. Boritz (2020). Are external auditors concerned about cyber incidents? evidence from audit fees. *Auditing: A Journal of Practice & Theory 39*(1), 151–171.

Liberti, J. M. and A. R. Mian (2008). Estimating the effect of hierarchies on information use. *The Review of Financial Studies 22*(10), 4057–4090.

Lin, C., S. Liu, and G. Manso (2020). Shareholder litigation and corporate innovation. *Mangement Science*.

Martinez Peria, M. S. and S. L. Schmukler (2001). Do depositors punish banks for bad behavior? Market discipline, deposit insurance, and banking crises. *The Journal of Finance 56*(3), 1029–1051.

Mester, L. J. et al. (2019). Cybersecurity and financial stability.

Nicoletti, A. (2018). The effects of bank regulators and external auditors on loan loss provisions. *Journal of Accounting and Economics 66*(1), 244–265.

Rosati, P., F. Gogolin, and T. Lynn (2019). Audit firm assessments of cyber-security risk: Evidence from audit fees and sec comment letters. *The International Journal of Accounting 54*(03).

Ross, D. G. (2010). The "dominant bank effect:" How high lender reputation affects the information content and terms of bank loans. *The Review of Financial Studies 23*(7), 2730–2756.

Skrastins, J. and V. Vig (2019). How organizational hierarchy affects information production. *The Review of Financial Studies 32*(2), 564–604.

Stein, J. C. (2002). Information production and capital allocation: Decentralized versus hierarchical firms. *The Journal of Finance 57*(5), 1891–1921.