Does Cybersecurity Slow Down Digitization? A Quasi-Experiment of Security Breach Notification Laws

Abstract

While digitization necessitates cybersecurity reforms, firms engaging in digitization initiatives may be discouraged by the costs of such major changes. Therefore, it has become increasingly important to understand if concerns about the costs of cybersecurity stifle digital growth. This study seizes an opportunity to address this question by investigating the state- and industry-level economic impacts of the passage of security breach notification laws (SBNLs) in United States, which act as legislative pressure in increasing the cybersecurity costs of digitization. We study the impact of SBNLs on an important economic topic – employment by IT service provider industry. Using a difference in difference design, we found that employment by mature IT service providers decreases following enactment of SBNLs. Impacts on younger IT service firms are not significant. The results hold under various robustness and falsification tests. This study provides fresh evidence related to the unintended and broader impacts of cybersecurity legislations.

Keywords: security breach notification law, IT service provider, employment, difference in difference

Introduction

Digitization, i.e., using information technologies (IT) and computational services to automate, streamline, and intelligize work processes and their end products, has been the cornerstone of economic growth and prosperity in the past two decades. At the same time, the uptake in digitization has coincided with the rise of cybersecurity breaches that target digital records and traces, and in many cases, threaten the economic viability of growing and established corporations alike. As such, identifying cybersecurity breaches and handling them effectively has become a key area of investment with a cost nature to shield corporations from the unintended consequences of digitization. Therefore, organizations undergoing digitization efforts are continually faced with a difficult question: do the costs of dealing with the rising cybersecurity threats turn digitization efforts to less attractive options? For the policy makers concerning digital development, the question morphs into whether or not the costs of dealing with cybersecurity threats set entry barriers for digitizing entities and stifle digital growth.

A straight-forward answer to the above questions is hard to obtain at a corporate level because identifying cancelled or reduced-in-size plans of digitization, as well as understanding the internal cost-benefit calculus behind such plans, is cumbersome due to a lack of detailed public records. However, legal changes triggering an increase in cybersecurity expenditure provide an opportunity to find some answers for those questions. This study capitalizes on one such opportunity.

By the end of 2018, all states in the US have passed security breach notification laws (SBNLs), requiring organizations to notify consumers and other entities[1] regarding breach of personal identifiable information. While SBNLs reduce risks for consumers (Kwon and Johnson 2014; Romanosky et al. 2011) and shareholders (Ashraf and Sunder 2018), the imposed compliance costs on organizations could incur barriers for digitization initiatives. These barriers may be magnified by the increased cyber-threats (Sen 2018) and the shortage of cybersecurity talents (Zadelhoff 2017). It is therefore important opportunity to understand the broader questions discussed above by studying how SBNLs affect digitization. Since the main procurers of digitization are IT service firms and employment is a fundamental indicator of economic dynamism for them, e.g., a slow-down, stagnation, or growth, (Bravo-Biosca et al. 2016), we focus on the influence of SBNLs on the increase or decrease in employment by IT service industries.

SBNLs will impact IT service firms in several ways. On one hand, mandatory reporting requirements further expose organizations to financial and reputational loss associated with data breaches. Firms with existing digital infrastructure

[1] Other notification entities typically include state attorney generals, consumer report agencies, third-parties that own the data.

will be incentivized to increase cybersecurity budgets, thus creating jobs for cybersecurity firms, a subset of IT service providers. Enhanced security will also boost consumer trust in digital goods and services, thereby benefiting general IT service providers. On the other hand, cybersecurity requirements could create barriers for digitization. Organizations will be discouraged from engaging in new digitization initiatives or expanding existing ones, and thereby destructing jobs for general IT service providers. In addition, the severe shortage of cybersecurity labor (Zadelhoff 2017) will limit organizations from engaging in digitization initiatives even when they are economically viable. The increased entry barrier to digitization will therefore negatively influence employment of IT service providers. With competing influences, this study empirically examines how enactment of SBNLs affect employment of IT service providers (RQ).

We exploit the staggered passages of state-level SBNLs, i.e., passages that happen at different points of time, to identify their effect on employment of IT service providers. Using a difference in difference design, we found that enactments of SBNL reduce employment for larger and more mature IT service firms, but has no effect towards smaller and younger firms. The main results are obtained after controlling for various state-level economic variables (unemployment rate, personal income growth rate, housing price index). Since our analysis suggests state economic and political conditions do not predict the passage of the laws, SBNLs enactments can be viewed as an approximate random assignment. Several robustness checks were conducted by including controls such as local sentiments about data breaches and the number of compromised records, and excluding data around the 2008 financial crisis, as well as data from California and Massachusetts, where IT industries are more vibrant. To further alleviate identification concerns, we tested the main model using a placebo timing and a placebo industry.

This paper appeals to three groups of audience. First, the study will add to the economics of digitization literature, which have traditionally focused on cost reduction through digitization (Goldfarb and Tucker 2019). While cybersecurity evidently adds cost to digitization, the issue lies in measuring its impact on the digital economy. The staggered passage of SBNLs provides a unique opportunity to identify the impact of cybersecurity on digitization. We show that the raised cybersecurity standards may become entry barriers for digitization, as reflected by the employment reduction of larger and more mature IT service providers. While prior literature have revealed social costs of digitization (Chan and Ghose 2013; Chan et al. 2019), this study explores the economic cost of digitization.

Second, this paper adds to the cybersecurity literature by revealing the economic implications of legislative mitigation strategies. Prior cybersecurity literature have shown that SBNLs reduce security breaches (Kwon and Johnson 2014; Romanosky et al. 2011), whereas the broader, perhaps unintended, economic impact of such legislations is virtually unexplored. With cyber threats becoming more severe (Sen 2018), an emerging literature focuses on whether cybersecurity investments can effectively prevent data breaches in key industries, such as the healthcare industry (Angst et al. 2017; Kwon and Johnson 2013; Kwon and Johnson 2014; Kwon and Johnson 2018). This paper takes a different focus and quantifies the economic impact of variation in the regulatory environment of cybersecurity investments.

Third, this paper will shed light on legislative discussions regarding cybersecurity. Similar discussions exist around other privacy laws. For example, previous research unfolded that that the compliance cost associated with healthcare privacy laws discourages electronic medical record adoption in hospitals (Miller and Tucker 2011). We focus on a different set of state-level legislations and explore beyond the healthcare industry. While politicians face increasing consumer pressure in holding organizations accountable for data breaches, it is also important to understand the costs and benefits of these laws to the critical areas of economy such as employment. With all states now having passed SBNLs, this paper will add to the discussions of federal level SBNL.

The rest of the paper will proceed as follows. We will first provide some background of SBNLs, and show that state-level economic, political, and legal environments do not predict passages of SBNLs. We will then explain the data sources used in the study, IT service industries classifications, firm-age and size classifications, and measurement of various constructs. Specifications of the generalized difference in difference (DID) design will be discussed. The main analyses will be followed by various robustness and placebo tests. We will conclude with discussions of limitations and implications of the study.

Institutional Background

The state-level security breach notification law (SBNL) was first introduced in California in 2002. By the end of 2018, all states have passed some version of the law. Figure 1 depicts the number of years since the enactment till the end of 2018. All SBNLs require organizations to notify customers in a timely manner when their personal identifiable information is breached through the organizations. Many states impose hard deadline such as 30 or 45 days to notify the affected party after a breach is discovered. Notification channels include written notice, email, phone call, etc. Some states allow exemptions if after investigation the company can provide written proof that the security breach will not harm the consumers. Apart from notifying customers, SBNLs often include notifications to state attorney generals, consumer report agencies and third-parties that own the data. Most of these notifications are only necessary if the number of compromised records exceeds a certain threshold. Personal identifiable information (PII) in SBNLs include name, social security number, driver's license number, state ID number, account number, credit/debit card number, pin, passwords. Some states define PII more broadly to include medical information and biometric information (e.g. fingerprint). A few states allow private citizens to pursue civil litigations against the entities that fail to comply with SBNLs. Federal-level SBNL was proposed in 2015, but did not pass the congress.

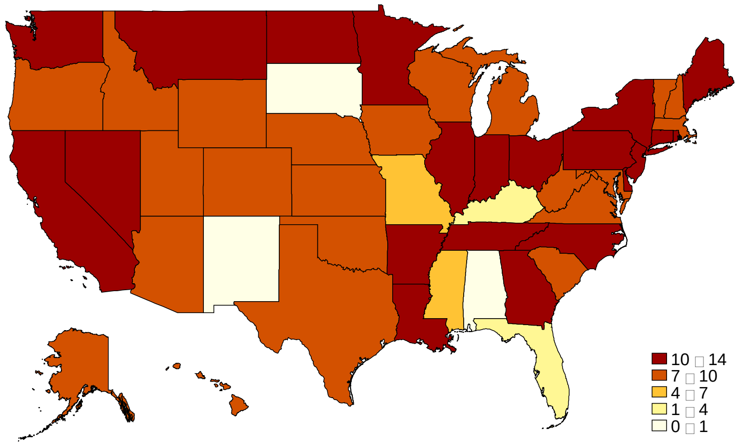


Figure 1. Years since Enactment of Security Breach Notification Law till the End of 2018

Needless to say, SBNLs were passed in order to mitigate cyber threats. More recent enactment of SBNLs may be partly due to the high-profile breach cases, such as the incident with Equifax in 2017. Because if the penalties associated with failure to comply, the passage of SBNLs puts a coercive institutional pressure on firms to update their cybersecurity practices or initiate new projects that enable compliance. Although the passage of SBNLs creates a suitable experimental context to study the impact of cybersecurity initiatives on the digital growth, a key question is whether or not the passage of those laws resemble a random assignment of treatment. Acknowledging that a full random assignment is far from the realities of policy making, our first step in the study was to ensure that the known factors influencing state policy did not systematically influence the passage of SBNLs.

Table 1 investigates whether a state's macroeconomic, political economy, or legal conditions predict the passage of SBNLs, following Appel et al. (2019). The SBNL dummy is set to one if the law is passed in the state, and o otherwise. The Democratic and republican control (Dem/Rep_State) dummies indicate the party controls both the legislative and executive branches. The dummies equal to 1 if both branches are controlled by the democratic/republican party, respectively, and equals to 0 for split controls. Legal ranking measures the business friendliness of the state legal system through the lawsuit climate survey conducted by the US Chamber of Commerce. Local sentiment of data breaches (GSV_Data_Breach) is measured by the Google search volume of the keyword "data breach". To avoid over-fitting, we did not include the state fixed effects in the logistic regression. The non-significant coefficients in Table 1 suggest that persistent state characteristics that correlate with the passage of SBNLs do not undermine the validity ofour difference-in-difference design. While treatments in quasi experiments are not randomized by and large (Angrist and Pischke 2009), the predictive regression suggests assignment of SBNLs is a decent approximation to randomization.

Table 1. Predictive Regression

	SBNL
Unemployment_Rate	0.053
	(0.29)
Personal_Income_Growth	-14.391
	(1.08)

Housing_Price_Index	0.005
	(0.94)
Dem_State	0.293
	(0.58)
Rep_State	-0.687
	(1.57)
Legal_Rank	-0.016
	(1.07)
GSV_Data_Breach	-0.769
	(1.09)
N	323

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Method

Data and Sample

State-level employment data is obtained from the Census Bureau's Quarterly Workforce Indicators (QWI). For each state-quarter, the QWI reports employment data is aggregated by firm age, size and four-digit North American Industry Classification System (NAICS). The QWI dataset divides firm age into five groups: 0-1, 2-3, 4-5, 6-10, 11+. In measuring the impact on employment, we collapse the firm age categories to three: 0-3, 4-10, 11+ years following (Appel et al. 2019), where firms aged 0-3 are considered startups. The QWI dataset divides firm sizes based on the number of employees: 0-19, 20-49, 50-249, 250-499, 500+. For symmetry with age categorization, we collapsed firm sizes into three categories as well: 0-49, 50-499, 500+.

To identify IT service industries, we follow the classification by the Census Bureau using the four-digit NAICS code (Haltiwanger et al. 2014) (see Table 2). The industry classification do not specify cybersecurity service providers. Signed and effective dates of SBNLs are collected from National Conference of State Legislatures (NCSL) and Perkins Coie. The sample period is from 2001 to 2016, one year before the first state SBNL enactment, and up to the latest QWI data availability. The main analysis with firm-age categorization has 3358 state-year-quarter observations. The sample size varies for subsequent analyses based on data availability. Computers and communication industries are used as a placebo in additional identification analyses.

Table 2. Industry classification

NAICS (2017)	Industry Description
IT Services	
5112	Software publishers
5191	Internet publishing and broadcasting
5182	Data processing, hosting, and related services
5415	Computer systems design and related services
Computers & Communications	
3341	Computer and peripheral equipment manufacturing
3342	Communications equipment manufacturing
3344	Semiconductor and other electronic component manufacturing
3345	Navigational, measuring, electromedical, and control instruments manufacturing
5179	Other telecommunications

Notes. The NAICS classification do not specify cybersecurity service providers. Internet services industries were treated as IT service providers. Computers & communications industries were used as a placebo industry in table 6.

Measures

The dependent variable, **employment** in IT service firms is measured as the natural logarithm of one plus the number of full quarter employment (emps in QWI), i.e., the number of jobs that are held on both the first and last day of the quarter with the same employer. Notably, employment by IT service providers includes but are not limited to IT labor. We use stable employments to measure the business dynamism of IT service industry. When an IT service provider has more business opportunities, it will hire more IT as well as non-IT staffs.

Our main explanatory variable, $\boldsymbol{SBNL_{st}}$, is an indicator set to one if SBNL has been signed into law in state s on or before year-quarter t, and zero otherwise. In a *pilot* study, we codified SBNLs based on the five dimensions in Ashraf and Sunder (2018): a) whether a notification law imposes a hard deadline following the discovery of a data breach; b) if a law requires firms to disclose data breach only if the breach is determined to reasonably likely to cause harm to the victims; c) if a law requires notification to the attorney general or other state agencies; d) if a law allows private citizens to pursue litigation against a firm that fails to comply with the data breach disclosure law; e) if a law defines personally identifiable information more broadly than general. While the codification is a more detailed depiction of the law, we found no significant effect towards IT employment in the main and robustness analyses, suggesting that passage of SBNL play a more dominant role than details of the law. The codification is hence omitted in subsequent analyses.

For control variables, we obtained state-level quarterly u*nemployment rate*, *personal income growth rate* from the Bureau of Economic Analysis (BEA). The *housing price index*, obtained from the Federal Housing Finance Agency[2], is measured by the average price changes in repeated sales or refinancing on the same properties. While the underlying assumption of natural experiments is that control and treatment groups have similar characteristics except for the treatment, it would be naïve to assume different states possess the unanimous economic background (e.g. Wyoming and New York). Hence, the three variables serve as controls for state-level economic conditions.

Specification

In an ideal experimental settings at the firm level, identical SBNL treatments would be randomly assigned to each individual firm, and employment at the firm level can be measured at different points in time, so that we can precisely identify how SBNLs affect different types of IT service providers over time. Needless to say, state-level laws are hardly randomly assigned (hence the predictive regression), and the employment measure is based on aggregated data at state and industry levels. With these restrictions in mind, analyses are conducted on a state-year-quarter level following a quasi-experimental design, where enactment of SBNL (treatment) is an approximation to random assignment (see Table 1).

We employ a generalized difference in differences (DID) specification at the state-year-quarter level following Bertrand and Mullainathan (2003). In this case, an event study would not accurately capture the effect of SBNLs due to lack of treatment and controls, whereas a simple DID specification would not be appropriate due to staggered nature of legislation enactments. Recent studies that involve staggered exogenous shocks have used similar specifications (Appel et al. 2019; Ashraf and Sunder 2018; Chan et al. 2019; Dhanorkar 2018). Our main analysis uses the following equation.

$$Employment_{st} = \alpha_s + \alpha_t + \delta \cdot SBNL_{st} + \gamma X_{st} + \epsilon_{st},$$

where α_s is a state fixed effect, which controls for state characteristics that do not vary over the sample period. α_t is a year-quarter fixed effect, which absorbs aggregate shocks affecting all states. X_{st} are control variables (state-level unemployment rate, personal income growth rate, housing price index). ϵ_{st} is an error term. In the above specification, the coefficient δ is the DID estimator of the effect of SBNL enactment towards employment of IT service firms.

This specification allows the same states to be part of the treatment and control groups at different points in time. The treatment group contains states passing a law at year-quarter t, i.e., the states experiencing the exogenous shock. The control group includes all states not passing a law at year-quarter t, regardless of whether they have or will pass a law (Angrist and Pischke 2009; Bertrand and Mullainathan 2003). This means the SBNL dummy may be equal to 1 and the state can still be in the control group. In essence, the generalized DID design can still produce a control group even when all states have passed the law, as long as the passage is staggered.

Analyses

The main results (Table 3) show that employment of IT service industries decreases following the passage of SBNLs relative to states not passing the laws, suggesting an adverse effect of SBNLs towards digitization. Column 1 and 5 show an overall decline across firm age and size groups. The two columns produced different coefficients because QWI, for privacy reasons, reports missing data when the employment number is low in each industry, and aggregating

---

[2] https://www.fhfa.gov/DataTools/Downloads/Pages/House-Price-Index-Datasets.aspx#mpo

employment data from different industries will introduce slight inconsistency in the employment data. Columns 2, 3, and 6 produced insignificant coefficients, suggesting that SBNL has no obvious impact on the employment by newer and smaller firms. The negative effect is significant for firms aged eleven years or older (column 4), and for medium and large firms with at least 50 employees (column 6 and 7), suggesting that the overall decline is driven mainly by larger and more mature firms.

This concentrated result on larger and mature firms is likely due to the fact that younger IT service firms are more risk-taking and agile relative to mature ones, and hence are more likely to swiftly cater to the portion of customer firms that keep their digitization projects with higher cybersecurity standards. Therefore, the results may suggest that supply of cybersecurity compliance services is concentrated in small and new firms, hence shielding them from the overall adverse impacts of a decrease in non-cybersecurity service demand.

Table 3. Main results

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Firm Age (Years since founding)				Firm Size (# of Employees)			
	All ages	0-3	4-10	11+	All sizes	0-49	50-499	500+
SBNL	-0.058**	-0.061	-0.033	-0.056**	-0.069*	-0.035	-0.098**	-0.119**
	(0.029)	(0.071)	(0.053)	(0.026)	(0.035)	(0.030)	(0.038)	(0.054)
Unemployment	-0.018*	-0.011	-0.001	-0.020*	-0.019*	-0.014*	-0.030	-0.023
	(0.009)	(0.017)	(0.015)	(0.011)	(0.009)	(0.007)	(0.019)	(0.019)
PI Growth Rate	0.366	0.244	0.418	0.455	0.290	0.106	0.056	-0.261
	(0.238)	(0.742)	(0.359)	(0.327)	(0.243)	(0.165)	(0.396)	(0.650)
Housing_Price	0.000	0.000	0.001	-0.000	0.000	0.001**	0.000	0.000
	(0.000)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,358	3,358	3,358	3,358	3,358	3,358	3,358	3,358
R-squared	0.995	0.971	0.980	0.992	0.994	0.996	0.981	0.906

*Notes. Robust standard errors clustered by state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively. PI growth rate stands for personal income growth rate.*

With results mainly driven by mature (age 11+) and large firms (number of employees 500+) in the main analyses, the robustness checks (Table 4) focuses on these firms exclusively. We found consistent results under various specifications and sample periods. In column 3, we controlled for the natural logarithm of one plus the number of compromised records (starting from 2005, from Privacy Rights Clearinghouse) in each state in year-quarter *t*, to ensure that levels of actual cyber threats, irrespective of legislative pressure, does not drive the findings. In column 4, we controlled for the local sentiment for breaches, measured by Google search volume (GSV) index for the search term "data breach" (starting from 2004). Since the 2008 financial crisis may have affected all 50 states unevenly, we excluded data from the last quarter in 2007 till the second quarter in 2009 (column 1), and test for post-crisis results (Column 2-4). As IT industries in California and Massachusetts are more vibrant, analyses excluding both states (Column 5) suggest the results are not driven by individual states. Finally, Column 6 reports weighted regressions with weights based on the natural logarithm of each state's employment in 2001, the first year in the sample. We also tested all main and robustness specifications using beginning of quarter and end of quarter employment (emp and empend in QWI, respecitively). The alternative employment measures produced very similar results[3].

To inspect the timeline of the impact of SBNLs, we added additional dummies in the main regression model (Table 5), where $SBNL[iQ]_{st}$ is set to one if SBNL is effective i quarters before year-quarter t for state s, and zero otherwise. We observe an increase in effect size following the event quarter, with the results concentrate on more mature and larger firms (see also Figure 2), similar to our main findings. It appears the effect is strongest at least four quarters after the events.

---

3 These results are available upon request.

Table 4. Panel A. Robustness check I. (Firm age=11+)

VARIABLES	(1) Exclude-Crisis	(2) Post-Crisis	(3) Post-Crisis	(4) Post-Crisis	(5) No CA&MA	(6) Weighted Regression
SBNL	-0.062**	-0.095*	-0.095*	-0.095**	-0.051*	-0.080***
	(0.026)	(0.048)	(0.048)	(0.047)	(0.027)	(0.025)
Unemployment	-0.020	-0.022*	-0.022*	-0.022*	-0.020*	-0.021*
	(0.012)	(0.011)	(0.011)	(0.011)	(0.011)	(0.012)
Personal_Income_Growth	0.572*	0.331	0.336	0.330	0.392	0.657
	(0.318)	(0.476)	(0.470)	(0.478)	(0.323)	(0.450)
Housing_Price	-0.000	-0.000	-0.000	-0.000	-0.000	0.000
	(0.000)	(0.001)	(0.001)	(0.001)	(0.000)	(0.000)
Ln(Data_Breach)			0.001			
			(0.001)			
GSV_Data_Breach				0.001		
				(0.002)		
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,008	1,719	1,719	1,719	3,259	3,358
R-squared	0.992	0.997	0.997	0.997	0.991	0.990

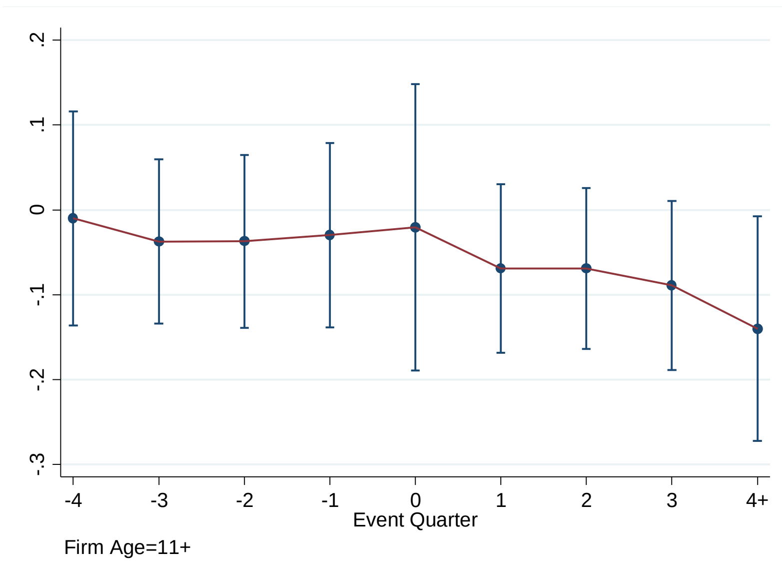
Panel B. Robustness Check II (# of Employees=500+)

VARIABLES	(1) Exclude-Crisis	(2) Post-Crisis	(3) Post-Crisis	(4) Post-Crisis	(5) No CA&MA	(6) Weighted Regression
SBNL	-0.131**	-0.168***	-0.168***	-0.167***	-0.109*	-0.133**
	(0.054)	(0.062)	(0.062)	(0.062)	(0.056)	(0.058)
Unemployment	-0.021	-0.024	-0.024	-0.024	-0.021	-0.031*
	(0.020)	(0.016)	(0.016)	(0.016)	(0.019)	(0.018)
Personal_Income_Growth	-0.219	0.319	0.344	0.320	-0.319	0.535
	(0.705)	(0.617)	(0.598)	(0.615)	(0.647)	(0.737)
Housing_Price	0.000	-0.000	-0.000	-0.000	0.000	0.001
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Ln(Data_Breach)			0.003			
			(0.003)			
GSV_Data_Breach				-0.001		
				(0.003)		
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,017	1,720	1,720	1,720	3,267	2,444
R-squared	0.898	0.965	0.965	0.965	0.912	0.985

*Notes. Robust standard errors clustered by state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively. Crisis is defined as the financial crisis from Q4 in 2007 to Q2 in 2009. CA and MA are short for California and Massachusetts. GSV_Data_Breach stands for the Google search volume index of "data breach" on the state level (starting from 2004). Column (6) reports weighted regressions with weights based on the natural logarithm of each state's employment in 2001, one year before the sample period.*

Figure 2 Evolution of Employment by IT Service Providers

The figures below plot the evolution of IT employment at mature IT firms (upper graph) and large IT firms (lower graph) in treatment groups relative to the control groups. The *y*-axis represents the coefficients on the dummy variables indicating the timing of breach notification law passage and the x-axis represents the event quarter centered around the quarter when breach notification law is signed (Event Quarter=0). The dots represent the point estimates and the vertical bars represent the 95% confidence intervals (see also table 5).



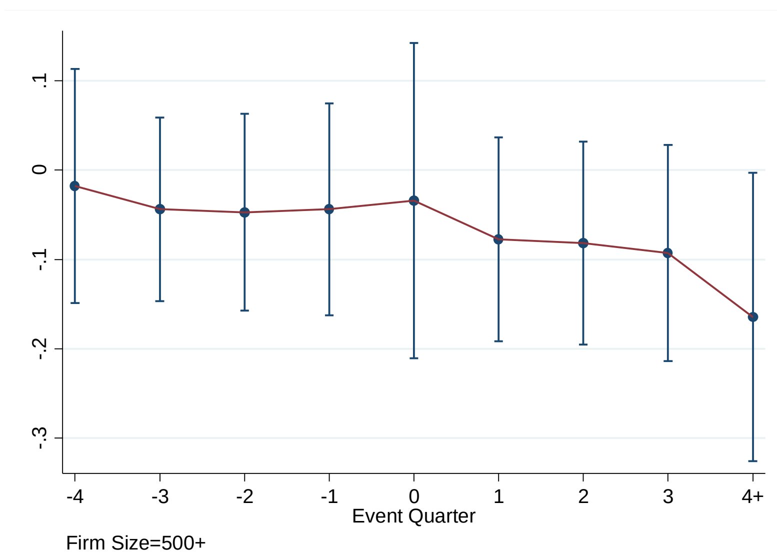


Table 5. Dynamic effects of security breach notification laws

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Firm Age (Years since foundation)				Firm Size (# of Employees)			
	All Ages	0-3	4-10	11+	All sizes	0-49	50-499	500+
SBNL[0Q]	-0.034**	-0.028	-0.018	-0.040**	-0.037**	-0.014	-0.032	-0.018
	(0.016)	(0.045)	(0.040)	(0.018)	(0.018)	(0.017)	(0.033)	(0.067)
SBNL[1Q]	-0.036**	-0.034	-0.031	-0.038**	-0.040*	-0.020	-0.055	-0.060
	(0.018)	(0.052)	(0.041)	(0.018)	(0.020)	(0.018)	(0.034)	(0.038)
SBNL[2Q]	-0.038*	-0.060	-0.022	-0.038**	-0.043*	-0.020	-0.069*	-0.058
	(0.019)	(0.054)	(0.046)	(0.018)	(0.022)	(0.020)	(0.036)	(0.039)
SBNL[3Q]	-0.044*	-0.043	-0.033	-0.047**	-0.050*	-0.031	-0.048	-0.079*
	(0.022)	(0.079)	(0.045)	(0.021)	(0.026)	(0.023)	(0.035)	(0.044)
SBNL[4Q+]	-0.074**	-0.074	-0.038	-0.072**	-0.089*	-0.043	-0.125**	-0.150**
	(0.036)	(0.086)	(0.067)	(0.033)	(0.044)	(0.038)	(0.048)	(0.066)
Unemployment	-0.018**	-0.011	-0.001	-0.020*	-0.019**	-0.014*	-0.031	-0.023
	(0.009)	(0.018)	(0.015)	(0.011)	(0.009)	(0.007)	(0.019)	(0.019)
PI growth rate	0.341	0.220	0.410	0.431	0.259	0.093	0.011	-0.309
	(0.240)	(0.735)	(0.361)	(0.327)	(0.249)	(0.169)	(0.403)	(0.653)
Housing_Price	0.000	0.000	0.001	-0.000	0.000	0.001**	0.000	0.000
	(0.000)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,358	3,358	3,358	3,358	3,358	3,358	3,358	3,358
R-squared	0.995	0.971	0.980	0.992	0.995	0.996	0.981	0.906

*Notes. Robust standard errors clustered by state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively.* $SBNL[iQ]_{st}$ *is set to one if SBNL is effective* i *quarters before year-quarter* t *for state* s*, and zero otherwise. PI growth rate stands for personal income growth rate.*

To further alleviate identification concerns, we also tested the main model using a placebo timing and a placebo industry (Table 6). Placebo timing is set at twelve quarters before the event (Column 1, 2) following Appel et al. (2019). The non-significant coefficients suggest the results are indeed due to enactments of SBNLs, and are not driven by other factors. Placebo tests with the false timing for other age and size categories produced similar non-significant coefficients, and are omitted in Table 6.

We chose computers and communications industry as a placebo since it is most similar to IT service industry (see industry descriptions in Table 2). Industry classifications follow Haltiwanger et al. (2014). Column 3-8 re-produced the main analyses using the computers and communication industries. Except for column 7, all coefficients are non-significant, suggesting that SBNL has no significant impact on employment of the placebo industry.

Overall, the results show no significant effect using either placebo, suggesting SBNL is the real driver in influencing employment of IT service industries. Finally, while the parallel-trends assumption in DID is ultimately untestable, there is some indirect evidence. We found no significant difference in the evolution of employment at treated and controlled states prior to the passage of SBNL (coefficients in Figure 1 before the event quarters are insignificant).

Table 6. Placebo tests

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Placebo Timing $= -12$		*Placebo Industry: Computers and Communications*					
VARIABLES	Firm Age =11+	Firm Size =500+	Firm Age 0-3	Firm Age 4-10	Firm Age 11+	Firm Size 0-49	Firm Size 50-499	Firm Size 500+
SBNL_Placeo	-0.077	-0.093						
	(0.051)	(0.060)						
SBNL			-0.074	-0.014	-0.011	-0.057	0.179**	0.052
			(0.124)	(0.139)	(0.057)	(0.052)	(0.086)	(0.087)
Unemployment	-0.026*	-0.022	0.008	0.026	-0.048**	-0.033	0.038	-0.097***
	(0.014)	(0.019)	(0.048)	(0.055)	(0.021)	(0.022)	(0.028)	(0.029)
Personal_Income_Growth	-0.222	-0.262	4.050**	0.408	-0.725	-0.607	2.008**	1.472
	(0.663)	(0.627)	(1.746)	(1.595)	(0.652)	(0.818)	(0.806)	(1.170)
Housing_Price	-0.000	0.000	-0.001	-0.002	-0.001	-0.002**	0.000	-0.009*
	(0.001)	(0.001)	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.005)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year-Quarter Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	3,358	3,358	2,863	3,058	3,367	3,291	3,194	3,361
R-squared	0.899	0.905	0.863	0.883	0.913	0.977	0.941	0.899

*Robust standard errors clustered by state are reported in parentheses. ***, **, and * denote significance at the 1%, 5%, and 10% level, respectively. Placebo timing is set to be 12 quarters before the event quarter. See Table 2 for descriptions of the placebo industry.*

Discussions and Conclusions

With the continuous increase in digitization activities coinciding with the rise of cybersecurity threats and costs of combating it, a lingering question has been one related to whether or not complying with institutional pressures of addressing cybersecurity threats hinders digital growth. Seizing an opportunity to conduct a natural quasi-experiment, this paper empirically measures the economic impact of enactment of security breach notification laws toward IT service industries. By exploiting the staggered passage of SBNLs, we employ a difference-in-differences design to identify the effect of SBNL enactment on the employment of IT service providers. The results show that passage of SBNLs significantly reduces employment for larger and more mature IT service providers, suggesting that digitization is slowed down by cybersecurity requirements.

Before discussing the implications of the study, we first acknowledge two limitations. First, inherent to the nature of DID design and limitations of aggregated data, the study does not provide explicit insights about the exact nature of employment dynamics in providers that cater cybersecurity services versus those who don't. As such, further firm-level scrutiny is required to better understand the nature of the overall decrease in IT service employment as a result of passing SBNLs.

The second limitation of the study is inherent to the state-level DID design, where we implicitly assumed different states are comparable without the SBNL shocks. This assumption can be challenged by comparing states with vastly different economic landscape (New York and Wyoming). While we have controlled for three macro-economic variables, there are likely other uncontrolled covariates. To better address the issue, future studies with employment data on more granular geographic levels, e.g., the county level, can form a better selection of treatment counterfactuals. While each state may not be entirely comparable, neighboring counties along state borders are very similar communities, where they experience SBNL shocks at different points in time.

Despite the limitations, this study has two implications for the literature. First, it adds to the economics of digitization literature that has traditionally focused on cost reduction through digitization. This study quantifies the added cost of digitization, i.e., cybersecurity. The advancement of digitization has vastly reduced the cost to search for, replicate, and transport data (Goldfarb and Tucker 2019). While these lowered costs create countless benefits, they also increase the exposure of sensitive data. To mitigate the threats, policy-makers introduced SBNLs to stimulate cybersecurity initiatives by firms. However, we have found evidence that in order to avoid the compliance costs of SBNLs, firms are deincentivized to engage in digitization, as reflected by employment reduction in service providers of digitization. The economics of digitization literature is closely related to the IS field as IT adoption and IT investment are both tied with digitization. As such, this paper serves as a bridge between cybersecurity literature and economics of digitization.

Second, this papers provides a new angle to the existing empirical cybersecurity literature. Behavioral security studies have addressed relationships between organizational risk mitigation mechanisms and psychological behavioral intentions (Bulgurcu et al. 2010; D'Arcy et al. 2009; Siponen and Vance 2010; Willison and Warkentin 2013). Firm-level cybersecurity studies largely focus on risk mitigation through cybersecurity investments (Angst et al. 2017; Kwon and Johnson 2018), as well as the value of cybersecurity investments (Bose and Leung 2019; Gordon et al. 2010). State-level cybersecurity study explores the effectiveness of cybersecurity legislations (Romanosky et al. 2011). This study relates to these prior studies since state-level cybersecurity legislations affect firm-level cybersecurity initiatives, which in turn influence individual level behavioral intentions. This paper differs from existing studies in that it focuses on the broader economic angle of cybersecurity. While digitization necessitates cybersecurity, we study how cybersecurity impact advancement of digitization on an aggregate level, through focusing the important indicator of employment.

For policy-makers, this study reveals the unintended consequences of SBNLs. The current debates of SBNLs center on whether certain provisions in the laws are effective in mitigating data breaches, and whether there is a need for a federal-level SBNL. This study sheds light on these discussions by providing a view of the unintended aspects of this legislation. Understanding the economic consequences of well-intentioned legislative agendas that affect firm-level cybersecurity initiatives on a larger scale is pertinent to the progress and advancement of such legislations.

References

Angrist, J., and Pischke, J.-S. 2009. *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton University Press.

Angst, C.M., Block, E.S., D'arcy, J., and Kelley, K. 2017. “When Do It Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches,” *MIS Quarterly* (41:3), pp. 893-916.

Appel, I., Farre-Mensa, J., and Simintzi, E. 2019. “Patent Trolls and Startup Employment,” *Journal of Financial Economics* (Forthcoming).

Ashraf, M., and Sunder, J. 2018. “Mandatory Disclosure of Cyber Incidents and the Cost of Equity.”

Bertrand, M., and Mullainathan, S. 2003. “Enjoying the Quiet Life? Corporate Governance and Managerial Preferences,” *Journal of Political Economy* (111:5), pp. 1043-1075.

Bose, I., and Leung, A.C.M. 2019. “Adoption of Identity Theft Countermeasures and Its Short-and Long-Term Impact on Firm Value,” *MIS Quarterly* (43:1), pp. 313-327.

Bravo-Biosca, A., Criscuolo, C., and Menon, C. 2016. “What Drives the Dynamics of Business Growth?,” *Economic Policy* (31:88), pp. 703-742.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS quarterly* (34:3), pp. 523-548.

Chan, J., and Ghose, A. 2013. “Internet’s Dirty Secret: Assessing the Impact of Online Intermediaries on Hiv Transmission,” *MIS Quarterly* (38:4), pp. 955-976.

Chan, J., Mojumder, P., and Ghose, A. 2019. “The Digital Sin City: An Empirical Study of Craigslist’s Impact on Prostitution Trends,” *Information Systems Research* (Forthcoming), pp. 1-20.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research* (20:1), pp. 79-98.

Dhanorkar, S. 2018. “Environmental Benefits of Internet-Enabled C2c Closed-Loop Supply Chains: A Quasi-Experimental Study of Craigslist,” *Management Science* (65:2), pp. 660-680.

Goldfarb, A., and Tucker, C. 2019. “Digital Economics,” *Journal of Economic Literature* (57:1), pp. 3-43.

Gordon, L.A., Loeb, M.P., and Sohail, T. 2010. “Market Value of Voluntary Disclosures Concerning Information Security,” *MIS Quarterly* (34:3), pp. 567-594.

Haltiwanger, J., Hathaway, I., and Miranda, J. 2014. “Declining Business Dynamism in the Us High-Technology Sector.”

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

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

Kwon, J., and Johnson, M.E. 2018. "Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance?," *MIS Quarterly* (42:4), pp. 1043-1067.

Miller, A.R., and Tucker, C.E. 2011. "Can Health Care Information Technology Save Babies?," *Journal of Political Economy* (119:2), pp. 289-324.

Romanosky, S., Telang, R., and Acquisti, A. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis and Management* (30:2), pp. 256-286.

Sen, R. 2018. "Challenges to Cybersecurity: Current State of Affairs," *Communications of the Association for Information Systems* (43:1), pp. 22-44.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly* (34:3), pp. 487-502.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS quarterly* (37:1), pp. 1-20.

Zadelhoff, M.v. 2017. "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It," in: *Harvard Business Review*.