Fool Me Twice? Data Breach Reductions through Stricter Sanctions

Joseph Buckman
Management Information Systems, Kansas State University

Matthew Hashim
Management Information Systems, University of Arizona

Tiemen Woutersen
Economics, University of Arizona

Jesse Bockstedt
Management Information Systems, Emory University

July 19, 2019

ABSTRACT

Data breach notification laws in the United States mandate firms to take remedial actions when consumer data is compromised. Interestingly, the policies contained within these laws vary by state and by year of law enactment. We investigate the effects of the various policies to determine how firms respond to the implementation of data breach notification laws. Drawing upon institutional and deterrence theory, we hypothesize that firms facing stricter sanctions resulting from a data breach will experience fewer subsequent breaches in comparison to other firms. We create a unique panel data set using breach information collected between 2005 and 2016 to estimate several panel regressions with fixed effects. Our results show that policies that increase the costs associated with a data breach reduce a firm's subsequent breaches by up to 50%, depending on the policy. Our findings are consistent across several robustness models and offer unique theoretical contributions to the information security literature as well as practical contributions to policymakers and security experts.

Keywords: data breach, deterrence, information security, econometrics, panel data

Acknowledgments: We thank Miriam Arden for her excellent research assistance. Comments are welcome, woutersen@email.arizona.edu.

1. INTRODUCTION

Regulators implement notification laws requiring organizations to release information about important events and practices they may otherwise be unwilling to disclose publicly. This promotes consumer awareness and change within the firm (Schwartz and Janger 2007). Notification laws thus empower consumers with information, allowing them to alter their behaviors, if desired, to minimize their unwanted risk. For example, the U.S. Safe Drinking Water Act (SDWA) defines water quality standards for community drinking water systems and requires public notification of violations due to contaminants. Accordingly, consumers respond to notification of contaminated drinking water, and engage in avoidance behavior such as increased consumption of bottled water (Zivin et al. 2011). We show empirically that—just as the SDWA raises consumer awareness and reduces the negative impact of contaminated water—stricter sanctions resulting from a data breach decreases the number of subsequent data breaches.

Firms collect, store, and leverage large amounts of consumer data to help them find a competitive advantage in the information-driven economy (Acquisti et al. 2015). Unfortunately, these activities also entice malicious actors to gain unauthorized access to collected data. Such data breaches partially offset the advantages firms derive, and more importantly, introduce consumers to potential harm (Spiekermann et al. 2015).[1] Because of the increased consumer risk, legislators have enacted data breach notification laws requiring firms to publicly disclose breach incidents and subjecting firms to punitive consequences. As a result, regulatory agencies often require firms to notify affected consumers of the breach, to provide a minimum duration of consumer identity theft protection, and to suffer the financial consequences of any fines assessed

[1] A data breach is an "incident or crime in which an individual's name plus their Social Security number, driver's license number, medical record, or financial record is put at risk because of exposure" (Identity Theft Resource Center 2016).

by regulators (Romanosky and Acquisti 2009). Besides direct financial consequences, firms also face consumer scrutiny and negative market consequences following the public notification of a data breach. These long-reaching consequences take months to normalize, damage brand image, reduce stock market valuation, and lower firm performance (Leonard and Rubin 2006, Acquisti et al. 2006, Ko and Dorantes 2006, Gatzlaff and McCullough 2010, Gordon et al. 2011). Consequences escalate even further for firms that experience multiple data breaches as the average financial impact of a breach increases from $4 million for an initial breach to nearly $10 million for a subsequent breach (Romanosky 2016).

The first instance of a breach notification law in the U.S. was the California Civil Code Section 1789.29, introduced in 2003, which requires firms to notify residents when their personal data is affected by a breach. Other states were slower to enact their own breach disclosure laws until a legislative turning point following a breach incident in 2008 at ChoicePoint (Gatzlaff and McCullough 2010).[2] As of 2018, all fifty states have enacted a breach notification law; however, the policies and consequences vary by state. Some researchers have already considered the effects of enacting a breach notification law within a state. Romanosky et al. (2011) found that the presence of a breach notification law within a state reduces the risk of identity theft within the state. Enacting a data breach notification law was also shown to affect the inter-breach time across various industries (Sen and Borle 2015). However, the literature has largely overlooked two fundamental aspects: (1) policies within data breach notification laws vary across states; and (2) laws are enacted at different points in time.

Our objective in this paper is to identify the effects of the different policies within a data breach notification law on the subsequent breaches firms experience over time. We recognize

[2] ChoicePoint is a data aggregation company that held billions of consumers' private information records.

five policies consistently addressed within data breach notification laws across the U.S. Based on institutional and deterrence theories, we hypothesize that policies with stricter sanctions will affect the number of subsequent breaches experienced by a firm. We empirically test our hypothesis with a unique panel data set containing data from 2005 through 2016 for all reported data breaches and state-level policies at the time of breach. We use observed initial breaches for sample selection and establish a quasi-natural experiment using panel regression models with fixed effects. The results support our hypothesis and indicate that stricter sanctions affecting the cost of a data breach reduces the number of subsequent breaches firms experience by up to 50%, depending on the policy. Additionally, we find that the effects of policies with stricter sanctions persist when we control for the number of consumers compromised in a breach. Our results show that increasing the costs associated with a data breach increases information security efforts within the firm, thereby lowering the firm's number of subsequent breaches.

2. THEORETICAL BACKGROUND

Institutional theory states that firms behave in accordance with the social and cultural forces within their environment (DiMaggio and Powell 1983). In the context of information security, regulators have created an institution that involves securing consumers' private information by enacting data breach notification laws (Laube and Bohme 2016). An institution is defined as a social structure comprised of normative and regulative elements governed by a system of authority that, over time, establishes stability and guidelines in organizational behavior (Scott 2001). Firms operating within the boundaries of the institution gain legitimacy (i.e., social acceptance from peers and stakeholders) and continued participation within the social environment (Scott 2008; Angst et al. 2017). Firms typically uphold the institution because

conformity may result in greater legitimacy and resources, whereas failure to uphold the institution may lower legitimacy and resources (Meyer and Rowan 1977).

Data breach notification laws institutionalize the security of private information by requiring firms to disclose malicious or incidental lapses in information security, thereby lowering firms' legitimacy within the environment in which they operate. Supporting evidence can be found throughout the data breach notification literature. For instance, Arora et al. (2008; 2010) demonstrate that firms operate in a less than socially optimal manner for addressing software vulnerabilities unless those vulnerabilities are publicly disclosed. Laube and Bohme (2016) argue that the direct penalizations and indirect penalizations that firms experience due to breach regulations affect their incentives to invest in preventive information security measures. Direct penalizations are penalties handed down by an overseeing agency such as fines and lawsuits, and indirect penalizations are consequences from direct penalization such as drops in stock valuation, consumer backlash, and poor firm performance.

Regarding indirect penalizations, evidence shows that firms adjust their data security practices following breach notification because of public backlash (Schneider 2009; Sen and Borle 2015). Firms' efforts toward quality remediation and openness to consumers in the post-breach period calms consumers' fears and doubts regarding continued usage (Choi et al. 2016) and helps normalize legitimacy among stakeholders. Recent high-profile cases include the 2013 Target and 2014 Home Depot data breaches, in which the cumulative costs for both companies exceeded $550 million (Daley 2016b). Target's 2013 breach resulted in stolen credit cards, damaged reputation, and loss of firm value, among other consequences. As a result, Target was among the first U.S. adopters of EMV Chip-and-PIN technology for payment processing, which is a strong countermeasure against credit card data theft. Given the principles of institutional

theory and firms' responses to breach notification, we argue that regulatory consequences are the primary incentive for the active prevention of data breaches.[3] Institutions are capable of influencing firm behavior through regulatory mechanisms (Boxenbaum and Jonsson 2008; Bjorck 2004).

Institutional noncompliance often leads to sanctions against the firm. Deterrence theory is commonly used to study sanction rhetoric in regard to information security, and provides that an actor can be dissuaded from a behavior by enforcing strong disincentives associated with the behavior (Wall et al. 2015). The theory states that firms are aware of the punishments and benefits associated with legislative policies and abide by those policies when the punishment exceeds the benefits (D'Arcy et al. 2009). Seminal studies that apply deterrence theory to information security behavior include Straub (1990) and Straub and Nance (1990), which found that salient behavior expectations and stringent punishment upon failure to meet those expectations reduced computer abuse. Evidence from IS research demonstrates the theory's usefulness in explaining security policy compliance (Johnston et al. 2015). Specifically, direct sanctions against the actor decreases misuse intentions (D'Arcy and Devaraj 2012; D'Arcy et al. 2009), increases security compliance (Siponen et al. 2007; Johnston et al. 2015), and improves the overall effectiveness of information security (Kankanhalli et al. 2003). Studying the outcomes related to information security policy, provided the policies are supported by an authoritative source, offers insight into the policy's ability to support an institution (Johnston et al. 2015).

[3] Conventional reasoning for institutional success also offers firm performance as a possible motivator. However, we argue firm performance is unlikely to affect active breach prevention due to misaligned incentive structures reported within the information security literature. See Anderson and Moore (2006) for a detailed discussion.

We extend deterrence theory to breach notification laws and the institution of securing consumers' private information. Policies within the laws vary across states; however, overseeing regulatory entities monitor the notification process to ensure the policies are upheld. For the purposes of our research, we exploit the fact that policies between states differ significantly in their sanctions. Some states enact policies with weaker sanction rhetoric (e.g., allowing notification exemptions), while other states enact policies with stringent sanction rhetoric (e.g., further financial penalty in addition to direct notification costs). Therefore, we posit that institutional pressure arising from the direct and indirect penalizations due to a prior breach, in conjunction with policies imposing harsh financial penalties, deter firms from experiencing subsequent data breaches.

To further illustrate the effects of harsh financial penalties from stringent sanctions, consider a firm with a profit function $\pi(cost, effort)$ that depends on the *cost* of a data breach and the *effort* to prevent this breach:

$$\pi(cost, effort) = K - \Pr(effort) * cost - effort,$$

where $\Pr(effort)$ is the probability of a breach that depends on *effort*, and *K* is a constant. Several studies in the IS literature have investigated the effects of increasing information security resources on IT security incidents and discovered that greater security resources led to fewer incidents (Straub 1990; Kwon and Johnson 2013; 2014). Therefore, increasing information security efforts decreases the probability of a data breach, causing the first derivative of $\Pr(effort)$ to be negative. Generally, a firm will first engage in low-effort tasks to reduce the probability of a breach. Once the firm has exhausted its low-effort tasks, the firm may expand to more effort-intensive tasks. Because the marginal effect of *effort* is decreasing, the second

derivative of $\Pr(effort)$ is negative. Assuming the firm is profit maximizing, the derivative of $\pi(cost, effort)$ with respect to *effort* is zero. This first order condition implies:

$$\Pr'(effort) = \frac{-1}{cost},$$

where $\Pr'(effort)$ denotes the derivative of $\Pr(effort)$ with respect to *effort*. As discussed above, the derivative is decreasing (in absolute value) in *effort*. The first order condition holds true, as increases in *cost* leads to increases in *effort*. Thus, a policy change that increases the *cost* of a data breach implies that the *effort* of the firm will increase, thereby decreasing the number of breaches experienced by the firm. Formally, we hypothesize the following:

Hypothesis: Firms that face stricter sanctions resulting from a data breach will experience a lower number of subsequent breaches in comparison to other firms.

3. DATA

To test our hypothesis, we create a unique, unbalanced panel data set of U.S. firms by combining breach data recorded between 2005 and 2016 by the Privacy Rights Clearinghouse (PRC) with state-level data breach notification policies. PRC is a non-profit organization that records data breach information from government agencies and news media websites when they are made public. PRC has been gathering breach information since 2005 and has grown into one of the largest and most comprehensive breach data sets available (Edwards et al. 2016).

We establish our panel through a series of steps. First, we generate a unique firm identification number according to the firm's name and the state in which the breach occurred. It is necessary to record the firm-state combination because in some instances large firms experienced multiple data breaches in different states. We take a conservative approach by assigning two different firm identification numbers, one for Firm A in state X and one for Firm

A in state Y, to treat the breach observations as occurring at two separate firms.[4] It is important to acknowledge that breach notification is dependent upon consumer residency rather than breach location. Therefore, firms with consumers spanning large geographic areas may comply with a breach notification law outside of the state in which the breach occurred. However, we argue that the use of the breach location state remains relevant and useful in determining the applicable notification law for several reasons. A majority of breaches during the observational period (91.6%) occur at small to medium-sized businesses or local organizations (e.g., hospitals and public education facilities) that may be less likely to extend their consumer base across state lines. Also, among the 4.6% of firms that experienced breaches in multiple states, many of the breaches were among franchises or retail branches of larger corporate entities. In many cases, franchises and smaller organizational branches have been slow to migrate toward holistic organizational data approaches, and predominantly housed local consumer data during our observational period (Daley 2016a). Therefore, it is more accurate to differentiate between breach locations by the same firm.

The second step in establishing our panel data set is to lengthen the panel with firm-year observations that extend from the year of initial breach to the end of the observational period, 2016. Doing so provides additional repeated measures within the observational period and captures changes in breach notification policies over time. The structure of the PRC data set limits the estimation techniques available, because many firms experienced a single data breach. Analytical methods using panel data, particularly fixed effects methods, often require a minimum of two firm-year observations to estimate within-firm differences.

[4] Treating the breach observations in this manner emphasizes caution because it could only lessen the effect of our policies in the analysis.

The third step is the removal of the initial breach observation from the panel to address self-selection bias. Our data set is self-selected because it consists of firms that have experienced one or more data breaches, and not all U.S. firms. We accordingly use individual fixed effects because the subset of firms in the PRC data may contain certain characteristics that predispose them to a data breach. The selection into our data set can depend on these fixed effects in an arbitrary and unrestricted way. Moreover, the explanatory variables, including policy variables, can be correlated with these fixed effects.

Examples of our panel data include the following. Firm A experiences a single data breach in 2013. Firm A has three firm-year observations in the panel (i.e., 2014, 2015, and 2016). Firm B experiences an initial data breach in 2013 and a second data breach in 2015. Firm B has three firm-year observations in the panel (i.e., 2014, 2015, and 2016). Firm C experiences an initial data breach in 2013 and a second data breach also in 2013. Firm C has four firm-year observations in the panel (i.e., 2013, 2014, 2015, and 2016)

The final data preparation step is combining the yearly time observation with the state in which the breach occurred to identify the policies enacted within the state's data breach notification law. We obtained policy information from the National Conference of State Legislatures, a bipartisan organization that has state legislative information to support government decision-making.[5] We identified five policies that were consistently addressed across breach notification laws (summarized in Table 1): 1) the exemption of notification when paper records are breached; 2) the exemption of notification when a firm can provide evidence that affected consumers are not at risk of being harmed in any way; 3) the exemption of notification when a firm can provide evidence that the data were properly encrypted; 4)

[5] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, last visited July 12, 2019.

requirement for firms to provide notification to the state attorney general; 5) allowance for consumers to file civil and/or criminal penalties against the firm in addition to penalties from an overseeing agency. The *Exemption Policies* may weaken the incentives of a firm to prevent subsequent breaches, while the *Private Right of Action* strengthens these incentives. Requiring that firms *Report to the Attorney General* is neither an obvious weakening nor strengthening of the incentives, and we added it to the analysis as a control. If the breach incident occurred prior to a state's implementation of a notification law, all policy fields were set to zero because a law had not yet established any policies. Table 2 provides a pairwise correlation matrix for the variables and illustrates that data breach notification laws containing policies with stricter sanctions (e.g., Private Right of Action) are less likely to be paired with weaker sanctions (e.g., Risk of Harm Exemption). Summary statistics are presented in Table 3.

Table 1. Summary of Policy Descriptions

Policy	Description
Weaker Sanctions	
Paper Exemption	Firms are exempt from data breach notification in the event that paper records are compromised.
Risk of Harm Exemption	Firms are exempt from data breach notification in the event a firm can prove that affected consumer are not at risk of being harmed.
Encryption Exemption	Firms are exempt from data breach notification in the event a firm can prove that the compromised data was properly encrypted.
Stricter Sanction	
Private Right of Action	Affected consumers may file civil and/or criminal penalties in addition to sanctions filed be an overseeing entity.
Control	
Attorney General Notification	Firms must provide data breach notification to the state Attorney General's office.

Table 2. Pairwise Correlations

	1	2	3	4	5	6
1 Breach$_{it}$	1.000					
2 Paper Exemption	0.007	1.000				
3 Risk of Harm Exemption	-0.015	0.479*	1.000			
4 Encryption Exemption	0.031*	0.151*	-0.007	1.000		

5 Private Right of Action	0.001*	-0.207*	-0.300*	0.032*	1.000	
6 Att. Gen. Notification	0.010	0.285*	0.230*	0.334*	0.207*	1.000

Note. n = 24,872, * $p < 0.001$.

Table 3. Summary Statistics

	Mean	St. Dev.	Min	Max
Breach_{it}	0.036	0.218	0	4
Paper Exemption	0.154	0.361	0	1
Risk of Harm Exemption	0.442	0.497	0	1
Encryption Exemption	0.731	0.444	0	1
Private Right of Action	0.214	0.410	0	1
Attorney General Notification	0.493	0.500	0	1

4. ANALYSIS AND RESULTS

In order to test our hypothesis that firms facing stricter sanctions resulting from a data breach will experience a lower number of subsequent breaches in comparison to other firms, we must first establish a rigorous identification strategy. Specifically, it is possible that other firm-specific characteristics affect the number of subsequent data breaches at a firm. Therefore, we use a fixed effects regression model to control for unobserved differences between firms, similar to random assignment in experimentation. The fixed effects specification enables a separate intercept for each firm, controlling for stable firm attributes that have minimal variation over time. The resulting panel model can be written as:

$$Breach_{it} = \beta Policies_{it} + \alpha_i + u_{it},$$

where $Breach_{it}$ is the number of breaches for firm identification number i in year t, $Policies_{it}$ is the vector of binary variables indicating the presence of each of the five policies within the state notification law in which firm i is located at time t, α_i is the firm fixed effect, and u_{it} is the

error term. We estimate the variation of u_{it} using robust standard errors to control for potential serial correlation in the time series.

Our model estimates yield interesting and useful results that support the effectiveness of stringent policy sanctions (Table 4, Model 1). We find that enacting the Private Right of Action policy significantly decreases ($\beta = -0.054,\ p = 0.004$) the number of subsequent breaches at a firm. Considering that the average number of subsequent breaches at the firms we observe is 0.108, our results demonstrate that allowing consumers to file civil and/or criminal penalties in addition to direct notification costs lowers the average to 0.054, representing a 50% decrease.

Table 4. Panel Regression with Fixed Effects

	(1)	(2)
Variable:	$Breach_{it}$	$Breach_{it}$
Paper Exemption	-0.037	-0.040
	(0.055)	(0.074)
Risk of Harm Exemption	-0.032	0.027
	(0.061)	(0.079)
Encryption Exemption	-0.086	-0.158†
	(0.074)	(0.095)
Private Right of Action	-0.054**	-0.094**
	(0.019)	(0.033)
Attorney General Notification	0.044	0.003
	(0.063)	(0.082)
*ln*Consumers		-0.033**
		(0.011)
Constant	0.108*	0.464**
	(0.050)	(0.121)
N	24,872	14,868
Firms	4,622	2,756
R^2	0.298	0.320
F	2.23*	3.39**

Note. † $p \leq 0.10$; $* p \leq 0.05$; $** p \leq 0.01$
Robust standard errors are reported.

In addition to estimating Model 1, we investigated if the effects persist when accounting for the size of the breach. Breaches of greater size may potentially confound the effects of a

policy due to increased cost and negative attention to the firm. That is, the increased cost and negative attention may motivate a firm to reduce subsequent breaches instead of policy. Accordingly, we use a subset of our panel to account for breach size by including the publicly disclosed number of consumers affected by a breach. Firms with an unknown number of consumers affected were excluded to avoid bias and unclear interpretation. We incorporate breach size into the panel using the natural logarithm of the earlier breach's size to address a skewed distribution resulting from the size ranging between 150 to over 1 million consumers. For example, suppose Firm A experienced an initial breach in 2014, affecting 1,000 consumers. The explanatory variable '*ln*Consumers' for the subsequent breach is then the natural logarithm of 1,000, i.e. 6.9.

Results of the fixed effects panel regression are shown by Model 2 in Table 4. Interestingly, the Private Right of Action policy effect persists when accounting for breach size and significantly reduces ($\beta = -0.094,\ p = 0.005$) the number of subsequent breaches experienced by a firm. The Encryption Exemption policy is marginally significant ($\beta = -0.158,\ p = 0.096$). Lastly, the number of consumers affected in the prior breach also significantly reduces ($\beta = -0.033,\ p < 0.004$) the number of subsequent breaches. Considering that the average number of subsequent breaches at the firms we observe is 0.464, our results demonstrate that the Private Right of Action policy lowers the average to 0.370 (a 20 percentage point decrease), the Encryption Exemption policy lowers the average to 0.306 (a 34 percentage point decrease). Further, if the number of customers increases by a factor of ten, then this lowers the number of future breaches by 8 percentage points.

Next, we estimate several models to check the robustness of our findings. First, we estimate a model that uses only two observations per firm. In particular, we estimate the

Arellano-Bond (1991) model (Table 5, Model 1). The Arellano-Bond model takes the first-differences and establishes a generalized method of moments to account for heterogeneity and correlation between regressors and the error term. We also estimate a panel regression with fixed effects and a linear time trend to control for time trends in data breaches (Table 5, Model 2). This table shows that our findings are robust against time trends. We find that the effects of the Private Right of Action policy persist across these alternative models, supporting our findings presented earlier.

Table 5. Robustness Tests

	Arellano-Bond	Time Trend
Variable:	$Breach_{it}$	$Breach_{it}$
Paper Exemption	-0.049	-0.036
	(0.083)	(0.055)
Risk of Harm Exemption	-0.107	-0.020
	(0.080)	(0.061)
Encryption Exemption	-0.059	-0.075
	(0.108)	(0.074)
Private Right of Action	-0.070**	-0.039*
	(0.026)	(0.019)
Attorney General Notification	0.159†	0.050
	(0.089)	(0.063)
$\text{Breach}_{i,t-1}$	0.026**	
	(0.006)	
Time Trend		-0.004**
		(0.001)
Constant	0.064	0.106*
	(0.070)	(0.049)
N	20,246	24,872
Firms	4,258	4,622
χ^2	27.68**	
R^2		0.299
F		7.61**

Note. † $p \leq 0.10$; $* p \leq 0.05$; $** p \leq 0.01$
Robust standard errors are reported.

5. DISCUSSION

Overall, our study offers a significant contribution to the information security literature by providing empirical evidence that firms improve their information security following a data breach when faced with stringent sanctions. Our results demonstrate the capability of regulatory intervention to improve information security among firms and to reduce the harm to consumers that are caused by these breaches. Further, our empirical approach and analysis offers insight into how the varying policies within data breach notification laws affect responses to a data breach. Specifically, enacting stricter policies that increase the cost of a data breach—e.g., the Private Right of Action policy—motivates firms to prevent a subsequent breach. We find that weaker policies—i.e. Exemption policies—do not have a negative effect on the number of future breaches.

We believe the broader implications of this finding yield several theoretical and practical contributions. First, offering notification exemptions may encourage efficient behavior among firms. For example, data encryption is a cost-effective, low-effort, countermeasure against a data breach (Ponemon Institute 2012). Firms residing in states with the Encryption Exemption policy may take advantage by initiating a baseline degree of effort through encrypting consumer data. However, once a minimal level of effort is achieved and exemption policy standards are met, the firm may perceive low value in continuing to pursue greater information security enhancement. Policymakers should therefore consider the institutional objective of data breach notification law when enacting exemption policies. If the objective is to incentivize low-effort firms to increase information security, an incentive structure that requires increased effort before exemptions are possible may be valuable. Conversely, if the objective is to generate continual advancement in information security within a firm, there may be a limited benefit to enacting exemption policies because firms do not receive further rewards for advancing beyond the exemption standards.

Under these circumstances, policymakers may consider supplying cost reductions according to the degree of security effort put forth by the firm.

Second, data breach notification policies affect the externalities of a breach. Firms form large networks with one another to share information and create value (Zhao et al. 2013). Growth in the firm network can yield benefits but may also introduce greater information security risk because of added entry points into the network. Malicious actors may gain access to other firms in the network after breaching an entry point. When considering the incentives of data breach policies on security efforts, exemption policies introduce a moral hazard. For example, suppose a network has several firms servicing consumers in different states. Firms with consumers in states that offer data breach exemptions have less incentive to invest in information security resources and accept greater breach risk from lower security effort. Consequently, the greater breach risk is distributed to the other firms in the network and forms negative externalities. On the other hand, firms with consumers in states that have enacted the Private Right of Action policy have a greater incentive to invest in information security resources and may expend increased security effort to reduce the breach risk distributed across the network. Hence, stringent sanction policies generate positive externalities.

Third, firms and IT management have historically struggled to justify information security investment and its benefits because of intangibility and difficult performance measurement (Anderson and Moore 2006). They argue that information security failure can be attributed to poorly designed incentive structures that do not affect firms following a data breach. However, our findings may demonstrate an institutional shift in the promotion of information security among firms. Data breach legislation that financially punishes a firm revises the incentive structure, aligning it with traditional economic reasoning and motivating security

investment. Experts can use our findings to illustrate the utility of information security resources to firm leaders and the importance of implementing such measures.

We acknowledge that our research is not without limitation. The use of the PRC data set may not offer an exhaustive list of all data breaches during the observational period. We are reliant on both PRC's methods and the truthfulness of the breach information firms provide. The number of breach observations in our panel may in fact be biased downward because of exemption policies allowing firms to forego notification, the absence of notification laws at the time of breach, or deceptive firm practices that hide a breach event. Under such circumstances, the firm-breach observation would fail to enter the panel. A second limitation to our panel is the lack of firm details. A majority of the breach observations in the panel occurred in privately owned firms, which provided minimal public information and limited the availability of additional variables. Future studies should consider investigating the small subset of publicly traded firms to identify discrepancies in firm size, to incorporate further control and treatment variables, and to explore their effects on subsequent data breaches.

6. CONCLUSION

In this paper, we find that data breach notification policies with stringent sanctions that increase the costs associated with breach reduce the number of subsequent breaches at a firm. Moreover, the introduction of exemption policies such as the 'Risk of Harm Exemption' do not affect the number of subsequent breaches at that firm. Our results further the information security literature because we are among the first to provide empirical evidence that firms likely alter their information security efforts in response to the implementation of stringent sanctions through data breach notification laws. The implications of our findings offer useful insight for future research on firms' information security efforts and actionable strategy for regulatory policymakers.

REFERENCES

Acquisti A, Friedman A, Telang R (2006) Is There a Cost to Privacy Breaches? An Event Study. *Proc. 27th Annual International Conference on Information Systems* (Association for Information Systems): 1563-1580.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* (347:6221): 509-514.

Anderson R, Moore T (2006) The Economics of Information Security. *Science* (314:5799): 610-613.

Angst C M, Block E S, D'Arcy J, 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): 893-916.

Arellano M, Bond S (1991) Some Tests of Specification for Panel Data: Monte Carlo Evidence and an Application to Employment Equations. *The Review of Economic Studies* (58:2): 277-297.

Arora A, Telang R, Xu H (2008) Optimal Policy for Vulnerability Disclosure. *Management Science* (54:4): 642-656.

Arora A, Krishnan R, Telang R, Yang Y (2010) An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure. *Information Systems Research* (21:1): 115-132.

Bjorck F (2004) Institutional Theory: A New Perspective for Research into IS/IT Security in Organizations. *Proc. 37th Annual Hawaii International Conference on System Sciences* (Institute of Electrical and Electronics Engineers).

Boxenbaum E, Jonsson S (2008) Isomorphism, Diffusion, and Decoupling. Greenwood R, Oliver C, Sahlin K, Suddaby R, eds. *The Sage Handbook of Organizational Institutionalism* (London: Sage), 299-323.

Choi B C F, Kim S S, Jiang Z (2016) Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems* (33:3): 904-933.

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

D'Arcy J, Devaraj S (2012) Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. *Decision Sciences* (43:6): 1091-1124.

Daley J (2016a) The Franchise World Finally Gets the Whole 'Big Data' Thing. *Entrepreneur* (January 8), https://www.entrepreneur.com/article/253837.

Daley J (2016b) Expenses from the Home Depot and Target Data Breaches Surpass $500 Million. *Digital Transactions* (May 26), https://www.digitaltransactions.net/ expenses-from-the-home-depot-and-target-data-breaches-surpass-500-million/.

DiMaggio P J, Powell W W (1983) The Iron Cage Revisited – Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review* (48:2): 147-160.

Edwards B, Hofmeyr S, Forrest S (2016) Hype and Heavy Tails: A Closer Look at Data Breaches. *Journal of Cybersecurity* (2:1): 3-14.

Gatzlaff K M, McCullough K A (2010) The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review* (13:1): 61-83.

Gordon L A, Loeb M P, Zhou L (2011) The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?. *Journal of Computer Security* (19): 33-56.

Identity Theft Resource Center (2016) Identity Theft Resource Center Breach Report Hits Near Record High in 2015. Report, Identity Theft Resource Center.

Johnston A C, Warkentin M, Siponen M (2015) An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly* (39:1): 113-134.

Kankanhalli A, Teo H H, Tan B, Wei K K (2003) An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management* (23:2): 139-154.

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

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

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

Laube S, Bohme R (2016) The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* (2:1): 29-41.

Leonard T M, Rubin P (2006) Much Ado about Notification. *Regulation* (29): 44-50.

Meyer J W, Rowan B (1977) Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology* (83): 369-391.

Ponemon Institute (2012) The Total Cost of Ownership for Full Disk Encryption. Report, Ponemon Institute.

Romanosky S (2016) Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity* (2:2): 1-15.

Romanosky S, Acquisti A (2009) Privacy Costs and Personal Data Protection: Economic and Legal Perspectives. *Berkeley Technology Law Journal* (24:3): 1062-1091.

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

Schneider J W (2009) Alternative Approaches to Deter Negligent Handling of Consumer Data. *Boston University Journal of Science and Technology* (15): 279-303.

Schwartz P, Janger E (2007) Notification of Data Security Breaches. *Michigan Law Review* (105): 913-984.

Scott W R (2001) *Institutions and Organizations*, 2nd ed. (Sage Publications, California).

Scott W R (2008) *Institutions and Organizations: Ideas and Interests*, 3rd ed. (Sage Publications, California).

Sen R, Borle S (2015) Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, (32:2): 314-341.

Siponen M T, Oinas-Kukkonen H (2007) A Review of Information Security Issues and Respective Research Contributions. *ACM SIGMIS Database*, (38:1): 60-80.

Spiekermann S, Acquisti A, Bohme R, Hui K (2015) The challenges of personal data markets and privacy. *Electronic Markets* (25:2): 161-167.

Straub D W (1990) Effective IS Security: An Empirical Study. *Information Systems Research* (1:3): 124-133.

Straub D W, Nance W D (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly* (14:1): 45-60.

Wall J, Lowry P B, Barlow J B (2015) Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations Under Conditions of Strain and Excess. *Journal of the Association for Information Systems* (17:1): 39-76.

Zhao X, Xue L, Whinston A B (2013) Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services and Risk Pooling Arrangements. *Journal of Management Information Systems* (30:1): 123-152.

Zivin J G, Neidell M, Schlenker W (2011) Water Quality Violations and Avoidance Behavior: Evidence from Bottled Water Consumption. *American Economic Review* (101:3): 448-453.