The Impact of Anti-phishing Laws on IT and Security Investment

Research-in-Progress

Xiaoxiao Wang **Wilson Weixun Li**

Alvin Chung Man Leung **Wei Thoo Yue**

Abstract

Many companies have been attacked by phishing leading to serious financial loss. In the United States, 23 states have enacted anti-phishing laws to ensure information security. However, the punishment rules of each state are different and the effects of the laws vary. Therefore, it is meaningful to study what kind of laws are the most effective to motivate firms to make appropriate IT and security investment decisions against phishing. Moreover, we posit that multi-site companies that operate in both with-law state and without-law state may have different IT and security investment decisions. We have collected 530 thousand corporates' investment data from 2010 and 2017. We plan to apply propensity score matching method and difference-in-difference model to answer our research questions. We hope that we can get some insights on developing effective anti-phishing laws and provide governments and regulatory agencies with some suggestions to motivate firms to adopt better anti-phishing solutions.

Keywords: Anti-phishing law, IT investment, security investment

Introduction

Phishing, a way to steal personal information by using fraudulent emails or websites, has caused serious financial loss for individuals and organizations. More than 60% of firms have experienced phishing attacks in the whole world (Admin 2018). A Symantec's report shows that phishing has caused more than 3 billion dollars loss for three years ("Internet Security Threat Report" 2017). In order to prevent phishing attacks, some security experts propose several strategies for firms to improve information security, such as installing antivirus software, using firewall services, and others. Apart from technical strategies, appropriate regulations and legislation may also deter phishing attacks. Prior research has shown that regulatory pressures can increase organizations' security awareness (Kwon and Johnson 2014; Sheng et al. 2009).

In the United States, though the federal government has implemented some laws to safeguard personal information, there is no federal law directly against phishing. The reason why federal anti-phishing law has not been passed may be that the effectiveness of anti-phishing laws varies across states. California was the first state enacting anti-phishing law in 2005. Up until now, there are about half of 50 states enacting anti-phishing laws to protect individuals' or organizations' information. As the state laws vary, firms' reactions to the laws also differ from one state to another. Therefore, it is important to study what kind of laws are the most useful to motivate firms to adopt appropriate IT and security measures against

phishing. This motivates us to implement this study to analyze the organizational reactions due to the passage of state-level anti-phishing laws. Furthermore, we can fully utilize the asymmetric enactment of anti-phishing laws in different states and compare firm behaviors in with-law states and without-law states.

The strictness levels of the anti-phishing laws vary from one state to another. We use the punishment severity of the anti-phishing laws as a proxy for the strictness level of the law. We also considered using other criteria to measure the strictness levels of the laws. However, these laws have similar definitions of phishing and defendant. In terms of punishments, some states' anti-phishing laws have more severe punishments to the offenders, while some do not clearly mention what kind of penalties will be applied to the offenders. Previous IS research summarizes the characteristics of phishing and details of different anti-phishing laws (Bose and Leung. 2007). However, prior studies do not investigate what characteristics of regulations are the most effective to deter phishing and motivate firms to adopt better anti-phishing measures. Aiming to fill this research gap, we conduct this research to examine how the varying levels of the strictness of anti-phishing laws influence firms' IT investment and security investment.

Instead of analyzing the impact of IT and security investment on a firm level, we examine it on a site level. A site refers to the business operations within a city of individual states. It may be a representation office of a firm or even a branch office of a firm. It should be noted that a firm may operate in multi-states. Therefore, we split all sample data into two types. One type is a firm that only operates its sites in states enacting anti-phishing laws. Another is a firm that operates sites in both states enacting anti-phishing laws and states without anti-phishing laws. The two types of firms may have different reactions after the enactment of state-level anti-phishing laws. The former group has no choice but to improve firms' information security to protect customers against phishing; the latter one may have an opportunity to shift firms' IT/security investment from with-law states to without-law states to shove off the responsibilities or punishment. We analyze the disparate reactions of different groups of companies.

We have constructed a panel data of thousands of sites in the United States. We plan to run a difference-in-difference (DID) model to examine different anti-phishing laws and their impacts on site-level IT and security investment. Because there are many external factors which may influence the investment decisions, for example, the size of sites and industrial factors, we use propensity score matching method (Xie and Lee 2015) to identify matching sites. These sites are owned by firms only operating in states without anti-phishing law. Then, we compare sites in with-law states and the matched sites by using the DID model. Lastly, we will perform some robustness checks to validate the parallel trend assumption of the DID model and results.

Literature Review

Our research aims to study how firms make their IT and security investment decisions as a response to anti-phishing laws. In this section, we review studies on anti-phishing and research examining IT investment and security investment decisions.

In IT investment and security investment studies, we focus on articles that investigate the relationship between IT-related investment and regulations or legislation. Menon and Lee (2000) study the influence of the diagnosis-related grouping (DRG) regulation on hospital IT use (Menon and Lee 2000). DRG regulation aims to achieve cost containment. The researchers found that the DRG regulation effectively motivates hospitals to decrease IT labor costs, while the DRG regulation shows slight effects on IT capital costs. Another study investigates how environmental regulations influence firms' technology choices (Gray and Shadbegian 1998). With consideration of the influence of the regulation strictness, the study finds that firms decrease the use of technology causing pollution when states' environmental regulation stringency is greater. In addition, some researchers study the access regulation in telecommunications market (Lestage and Flacher 2014; Manenti and Scial 2013). Lestage and Flacher (2014) compare the optimal access regulations under various stages of telecommunications market liberalization. They point out that the higher the access price, the more investment in infrastructures. Manenti and Scial (2013) find that access regulation may cause a negative impact on investment. In

addition, some articles examine information security related investment, while few focus on the influence of regulations. One research points out that the legislation in information security can improve firms' security awareness and security investment (Chai et al. 2011). In general, it seems that the implementation of the laws has realized their intended goals.

Previous researches examining how to make appropriate investment decisions primarily use analytical modeling method. Gordon and Loeb (2002) build an economic model of information security investment and use vulnerability as the index (Gordon and Loeb 2002). The vulnerability means the probability of the information set being attacked without additional security protection. The model shows that information security investment will increase and then decrease when vulnerabilities increase. The uncertainty of IT investment is emphasized in several articles (Fichman et al. 2005; Park et al. 2016). One tool used to solve the uncertainty is real options. Park et al. (2016) take emotions into consideration to provide a psychological understanding of IT real options. What's more, some researchers apply game theory and decision theory to determine IT security investment. However, their models are not suitable for phishing attacks (Cavusoglu et al. 2008) and their models have some assumptions that may not be applicable to the real world.

With regard to phishing in IS research, some researchers investigate why people believe in deceptive phishing emails or websites (Wright et al. 2014; Wright and Marett 2010) and the reasons of failure to detect phishing emails (Rao et al. 2018). Some researchers develop solutions for detecting phishing websites (Abbasi et al. 2015) and find appropriate training methods to avoid phishing attacks (Jensen et al. 2017). Nevertheless, there is a lack of research studying the impacts of anti-phishing laws. Our research aims to fill the gap and investigate how anti-phishing laws can increase organizations' security awareness and motivate them to make more appropriate IT and security investments decisions.

Hypothesis

The state-level anti-phishing laws were enacted to prevent the widespread of phishing attacks and safeguard customers' sensitive information. Although the laws do not mandate that firms should be obliged to take preventive actions, the regulatory pressure can increase firms' security awareness on phishing (Chai et al. 2011; Sheng et al. 2009). Therefore, with the enactment of the anti-phishing laws, we posit that sites will increase their IT investment and security investment.

H1: Anti-phishing laws motivate sites to increase IT-related investment and sites' willingness to purchase security-related software.

Anti-phishing laws vary in terms of punishments from one state to another. Offenders may include phishers and organizations. The organizations may be punished because they fail to safeguard customers' sensitive data or pay less effort to detect possible phishing activities originated from their domain networks. Punishments vary from fines to imprisonment. Although punishments take place after the occurrence of phishing, anti-phishing laws may still serve as a warning signal to the general public to stay alert to the online crime (Garfinkel et al. 2007). Based on the severity of punishments of different state laws, we divide our sample data into different groups. Among states with severe punishments, phishing-related activities (e.g., mass broadcast of phishing emails and hosting of phishing websites) are considered as a felony. Apart from paying fines, offenders may be subject to imprisonment. Lenient states with the anti-phishing laws usually have a vague description of phishing activities, and they usually consider phishing activities as misdemeanors and offenders are required to pay some fines. Hence, to avoid prosecution by the laws, we posit that sites operating in with-law states have a higher willingness to invest in IT and security than sites operating in states with more lenient anti-phishing laws.

H2: Sites operating in states with severe punishments are more likely to increase IT-related investment and willingness to purchase security-related software than sites operating in states with lenient anti-phishing laws.

As some companies operate in multiple states, they have an option to relocate a part of their business activities in some states. With the enactment of anti-phishing laws, some multi-state companies may actually shift some data sensitive operations from with-law states to without-law states. In case a

phishing incident occurs and some sensitive data are stolen, the company does not have to bear any legal consequences. Research finds that, if a firm may need to pay more costs due to the strict regulations, the firm will shift its production capacity to regions with lenient regulations (Dechezlepretre and Sato 2017). However, companies that operate only in states with anti-phishing laws, they may not have such flexibility. Therefore, we conjecture H3 as follows.

H3: Companies with sites in both with and without anti-phishing laws are more likely to reduce their IT-related investment and willingness to purchase security-related software than companies with sites operating in anti-phishing laws.

Data and Methodology

We obtain detailed IT and security investment data from Harte-Hanks Market Intelligence from 2010 to 2017, with more than 530 thousand organizations in the United States. During this period, some states enacted their anti-phishing laws, such as Illinois, Alabama, and so on. The data include each site's annual IT-related investment, current IT installed and future IT purchases. The IT-related investment includes general IT and security. We use the total IT budget and storage budget to measure IT investment. For the security investment, we use the purchase likelihood of security-related software to characterize the security investment. The definition and details of the measures are shown in Appendix Table 1.

In our study, we focus on sites that operate in states starting to enact anti-phishing laws after 2010. We use propensity score matching to identify control sites that are owned by firms only operating in states without the enactment of anti-phishing law. We identify sites of a company that operates in both states enacting anti-phishing laws and states without anti-phishing laws by an indicator variable "iftwo". It equals to 0 if a firm operates in a state with anti-phishing law only. We identify states with anti-phishing laws based on the reports of the National Conference of State Legislatures (NCSL). There are 23 states with anti-phishing laws and 27 states without anti-phishing laws up until now. All the 23 states' anti-phishing laws clearly define what kinds of behaviors are considered as phishing, who are responsible for financial loss generated by phishing and the legal liabilities of offenders. It should be noted that the penalties of different states vary. Some states, such as Alabama and Arizona, consider phishing as a felony. Apart from fines to recover the damages caused by phishing, the state laws also include imprisonment. However, some states, for example, California and Florida, consider phishing as misdemeanors and only require offenders to pay fines. Moreover, some states, such as Montana and Oregon, do not clearly specify what the punishments are. Hence, we use the punishment severity as a criterion to separate the states with anti-phishing laws into different groups. Then, we investigate whether different severity of the penalties can cause different impacts on IT and security investment. The details on the different levels of punishments in different states are shown in Appendix Table 2.

Research Plan

In the next stage of this research, we will perform the DID model to test our hypotheses. We will use "Antiph" as the treatment dummy and "timeD" as the time dummy (see Table 1). The interaction term "Antiph×timeD" captures the influence of anti-phishing law on investment. We will compare the impacts of anti-phishing laws with different punishment levels. In addition, we will investigate the differences of the investment decisions of companies that operate in both states with anti-phishing laws and states without the laws and companies only operating in states with anti-phishing law. In order to satisfy the parallel trend assumption of DID model, we will apply the propensity score matching method to match treatment group (i.e. sites in states with anti-phishing laws) with a control group that consists of sites in states without anti-phishing laws. This method can make sure that the treatment group and the matched control group have the same change trend before the law was published. The variables used in the matching process are also the control variables in the DID model, including the number of employees, the present installed software and so on (see in Table 1). The reason why we use these control variables is that the size of sites, revenue, and their currently installed security software may influence their subsequent investment decisions. Here is our DID model:

$$Dependent\ variables_{it} = \beta_1 Antiph_i + \beta_2 timeD_t + \beta_3 Antiph_i \times timeD_t + \gamma Control\ variables_{it}$$

We have four dependent variables measuring the site's IT-related budget and the purchasing likelihood score of security-related software. β_3 is the coefficient estimate of the treatment effect after the enactment of anti-phishing law in a state.

As the next step of the research, we will standardize all data such that we can compare the influence of anti-phishing laws with different strictness levels. Furthermore, in our robustness checks, we will check whether industry type (e.g., telecommunication industry and Internet service providers) will influence our results. The type is defined by the North American Industry Classification System (NAICS). Different types of business have different NAICS codes. We will examine whether the industry factor moderates the impacts of anti-phishing laws on firms' IT and security investment. In the main study, we compare firms only operating in states with anti-phishing laws implemented after 2010 and firms that operate in both states with anti-phishing laws implemented after 2010 and states without the laws. There are two other types of firms operating in multiple states. One type is firms with sites in states with anti-phishing laws enacted after 2010 and states with anti-phishing laws enacted before 2010. Another type is firms with anti-phishing laws enacted after 2010, states with anti-phishing laws implemented before 2010, and states without the laws. We will compare all four types of companies' IT and security investment decisions before and after the anti-phishing law was enacted to find more insights.

Our research may have several potential contributions. Firstly, we provide insights to understand the influence of the strictness level of anti-phishing law on IT and security investment. Previous studies do not examine the detail of the legislation or regulations on information security or the disparate organizational behaviors among firms operating in different states. We hope that our research can enrich existing literature by extending our knowledge in the fields of IT and security investment.

Secondly, our research results may be useful in practice. Because we use enormous data to analyze firms' behavior before and after the implementation of anti-phishing laws. Based on our results, we can provide some insights for governments or law-related agencies to evaluate existing anti-phishing laws in different states. Based on the results, they may develop better legislation that can encourage firms to adopt more proactive approaches to deter phishing.

Thirdly, our research may be one of the first studies investigating anti-phishing law s' impacts by using empirical methods in IS. We hope that we can provide some insights for future research, especially research on theorizing the impact of laws on organizational behaviors and firms' decisions on IT and security investment.

References

Abbasi, A., Zeng, D., Chen, Y., Chen, H., and Nunamaker Jr, J. F. 2015. "Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information," Journal of Management Information Systems (31:4), pp. 109–157.

Admin. 2018. "15 Alarming Cybersecurity Stats and Facts in 2018." (https://www.phreedom.com/it-security-trends/15-alarming-cybersecurity-stats-and-facts-in-2018/).

Anthony Byrd, T., Lewis, B. R., and Bryan, R. W. 2006. "The Leveraging Influence of Strategic Alignment on IT Investment: An Empirical Examination," Information and Management (43:3), pp. 308–321.

Bose, I and Leung, ACM. 2007. "Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities," Communications of the Association for Information Systems (19), pp. 544–566.

Cavusoglu, H., Raghunathan, S., and Yue, W. T. 2008. "Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment," Journal of Management Information Systems (25:2), pp. 281–304.

Chai, S., Kim, M., and Rao, H. R. 2011. "Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior," Decision Support Systems (50), pp. 651–661.

Dechezleprêtre, A., and Sato, M. 2017. The Impacts of Environmental Regulations on Competitiveness. Review of Environmental Economics and Policy, 11(2), 183-206.

Fichman, R. G., Keil, M., and Tiwana, A. 2005. "Beyond Valuation: 'Options Thinking' in IT Project Management," California Management Review (47:2), pp. 74–96.

Garfinkel, R., Gopal, R., and Thompson, S. 2007. "Releasing Individually Identifiable Microdata with Privacy Protection Against Stochastic Threat: An Application to Health Information," Information Systems Research (18:1), pp. 23–41.

Gordon, L. A., and Loeb, M. P. 2002. "The Economics of Information Security Investment," Advanced Materials Research (5:4), pp. 438–457.

Gray, W. B., and Shadbegian, R. J. 1998. "Environmental Regulation, Investment Timing, and Technology Choice," The Journal of Industrial Economics (46:2), pp. 235–256.

Huang, S.-M., Ou, C.-S., Chen, C.-M., and Lin, B. 2005. "An Empirical Study of Relationship between IT Investment and Firm Performance: A Resource-Based Perspective," European Journal of Operational Research (173), pp. 984–999.

"Internet Security Threat Report." 2017. (https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf).

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," Journal of Management Information Systems (34:2), pp. 597–626.

Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," Management Information Systems Quarterly (38:2), pp. 451–471.

Lestage, R., and Flacher, D. 2014. "Infrastructure Investment and Optimal Access Regulation in the Different Stages of Telecommunications Market Liberalization," Telecommunications Policy (38), pp. 569–579.

Manenti, F. M., and Scial, A. 2013. "Access Regulation, Entry and Investments in Telecommunications," Telecommunications Policy (37), pp. 450–468.

Menon, N. M., and Lee, B. 2000. "Cost Control and Production Performance Enhancement by IT Investment and Regulation Changes: Evidence from the Healthcare Industry," Decision Support Systems (30), pp. 153–169.

Park, E. H., Ramesh, B., and Cao, L. 2016. "Emotion in IT Investment Decision Making with A Real Options Perspective: The Intertwining of Cognition and Regret," Journal of Management Information Systems (33:3), pp. 652–683.

Rao, H. R., Li, Y., and Wang, J. 2018. "Overconfidence in Phishing Email Detection," Journal of the Association for Information Systems (17:11), pp. 759–783.

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L., and Hong, J. 2009. "Improving Phishing Countermeasures: An Analysis of Expert Interviews," 2009 ECrime Researchers Summit, ECRIME '09, IEEE, pp. 1–15.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. 2014. "Research Note-Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," Information Systems Research (25:2), pp. 385–400.

Wright, R. T., and Marett, K. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," Journal of Management Information Systems (27:1), pp. 273–303.

Xie, K., and Lee, Y. J. 2015. "Social Media and Brand Purchase: Quantifying the Effects of Exposures to Earned and Owned Social Media Activities in a Two-Stage Decision Making Model," Journal of Management Information Systems (32:2), pp. 204–238.

Appendix

The appendix shows the list of variables and the different punishment level of anti-phishing laws.

Definition of Variables

Table 1. Variables		
Type	Name	Definition
Treatment Dummy variable	Antiph	=1 if the site i is in a state with anti-phishing law.

Time Dummy Variable	timeD	=1 if the YearID is equal or larger than the year when the anti-phishing law was acted in certain state.
Control Variable (Treatment Independent Variable)	emple	The number of Employees
	reven	Estimated revenue
	IT_staff	The number of IT or IS employees.
	Internet_users	The number of employees using the Internet
	outsource_server_maint_pres	The likelihood of the third-party server maintenance being used at the site.
	outsource_hardware_maint_pres	The likelihood of the third-party hardware maintenance being used at the site.
	outsource_datacenter_mgmt_pres	The likelihood of the third-party data center management being used at the site.
	outsource_hardware_services_pres	The likelihood of the third-party hardware services being used at the site.
	outsource_disaster_recovery_pres	The likelihood of the third-party disaster recovery being used at the site.
	outsource_storage_mgmt_pres	The likelihood of the third-party storage management being used at the site.
	outsource_phone_maint_pres	The likelihood of the third-party phone system maintenance being used at the site.
	outsource_lan_services_pres	The likelihood of the third-party LAN management services being used at the site.
	outsource_wan_services_pres	The likelihood of the third-party WAN management services being used at the site.
	outsource_sw_services_pres	The likelihood of the third-party software services being used at the site.
	Idaccess_sw_pres	The likelihood of ID/Access software being used at the site.
	security_sw_pres	The likelihood of security software being used at the site.
	outsource_firewall_maint_pres	The likelihood of the third-party firewall services being used at the site.
	outsource_ids_maint_pres	The likelihood of the third-party Intrusion Detection Services (IDS) being used at the site.
	storage_capacity_expansion_pls	Purchase likelihood score of purchasing additional storage devices (i.e. NAS)
	storage	Gigabytes used for Storage
	IT_budget	The total IT budget

Dependent Variables	storage_budget	The storage budget
	security_sw_pls	The purchase likelihood score of security software (i.e. firewalls)
	antivirus_sw_pls	The purchase likelihood score of anti-virus software
Other Variables	iftwo	=1 means the site belongs to a firm that owns sites in states with the laws enacted after 2010 and states without the law; =0 means the site belongs to a firm that owns sites in states with the laws enacted after 2010.

The Strictness of the Anti-phishing Law

We use "Punishment" as a criterion to differentiate with-law states. "Punishment" refers to the degree of the strictness of punishment prescribed by the anti-phishing law. The range is 0 to 4. The table shows the detail.

Table 2. The Strictness Level of the Anti-phishing Law

Punishment	Felony with fine (4)	Only felony (3)	Misdemeanor with fine (2)	Only fine (1)	No clear rules (0)
States	Alabama; Arizona; Connecticut; Georgia; New Mexico; Rhode Island (AL, AZ, CT, GA, NM, RI)	Kentucky; Virginia (KY, VA)	Arkansas; Tennessee (AR, TN)	California; Florida; Illinois; Louisiana; Michigan; Minnesota; New York; Oklahoma; Texas; Utah; Washington (CA, FL, IL, LA, MI, MN, NY, OK, TX, UT, WA)	Montana; Oregon (MT, OR)