

**PROACTIVE VS. REACTIVE SECURITY INVESTMENTS
IN THE HEALTHCARE SECTOR**

Completed Research Paper

Juhee Kwon
Center for Digital Strategies
Tuck School of Business
Dartmouth College
Juhee.kwon@tuck.dartmouth.edu

M. Eric Johnson
Center for Digital Strategies
Tuck School of Business
Dartmouth College
m.eric.johnson@tuck.dartmouth.edu

Abstract

Building on organizational learning theory, we seek to identify the performance effects of security investments that arise from previous failures or external regulatory pressure. This study focuses on the healthcare sector where legislation mandates breach disclosure and detailed data on security investments are available. Using a Cox proportional hazard model, we demonstrate that proactive security investments are associated with lower security failure rates than reactive investments. Further, the results show that external pressure improves the security performance of healthcare organizations. However, external pressure decreases the positive effect of proactive investments on security performance. This implies that proactive investments, voluntarily made, have the greatest impact on security performance. Our findings suggest that security managers and policy makers should pay attention to the strategic and regulatory factors influencing security investment decisions. The implications for proactive and reactive learning with external regulatory pressure can likely be generalized to other industries.

Keywords: *Security investment, Organizational Learning, Proactive, Reactive, Healthcare*

PROACTIVE VS. REACTIVE SECURITY INVESTMENTS IN THE HEALTHCARE SECTOR¹

Introduction

In many areas of organizational performance, learning has been found to be an important element of performance improvement. Organizational learning, which explains how organizations acquire the knowledge and skills necessary to achieve better performance, has traditionally been used to examine decisions surrounding investments for quality and volume improvement in manufacturing (Dorroh et al. 1994; Fine 1986; Hatch et al. 1998; Ittner et al. 2001; Mukherjee et al. 1998; Salomon et al. 2008). A more recent organizational challenge is information security. With the steady escalation of information security breaches, organizations in every industry have struggled to learn how to defend themselves against an evolving set of threats. Recent large breaches of personal information in diverse industries from retail to gaming have increased public awareness of security failures and have no doubt contributed to identity theft and privacy violations.

In the healthcare sector, information security has long been a concern (Anderson, 1996), but has become a growing public interest as organizations increasingly move sensitive patient information into electronic medical records (EMR). Research has documented U.S. cases where patient information has been maliciously exploited by criminals seeking to commit medical and financial identity theft (Johnson 2009; Lohmeyer et al. 2002). The resulting public concern has fueled both federal and state legislation mandating breach notification (Roberds and Schreft 2009; Romanosky et al. 2011). Federal regulations like HIPAA² and HITECH³, as well as individual state regulations, now require providers to follow various notification guidelines to disclose

¹ *This research was partially supported by the National Science Foundation, Grant Award Number CNS-0910842.*

² *HIPAA : Health Insurance Portability and Accountability Act*

³ *HITECH : Health Information Technology for Economic and Clinical Health Act*

breaches. Such public notifications are costly and result in negative publicity (Kannan et al. 2007; Kolfal et al. 2010; Wang et al. 2008). Both legislation and breaches trigger investment and organizational learning (Gordon and Loeb 2006; Mulligan and Bamberger 2007). In this paper, we investigate the effects of security investments and external regulatory pressure on security performance. We do this in the context of the health sector, which provides a particularly appropriate context to investigate the impacts of voluntary and involuntary security investments.

The organizational literature has argued that investments in quality are often precipitated by failures or external mandates, and the investments result in organizational learning that ultimately yield performance improvement (Haunschild and Rhee 2004; Ittner et al. 2001; Salomon and Martin 2008). Ittner et al. (2001) investigated two separate learning effects from proactive and reactive investments that are decided by whether defects trigger investment. They argued that learning is a function of both proactive investments in performance improvement and autonomous learning-by-doing rather than a function of reactive investments alone.

Others in the organizational literature have examined how organizational performance interacts with external mandates, such as government regulations (Marcus and Nichols 1999; Naveh and Marcus 2004). Researchers have found mixed results. Some have found that external pressures are important for organizational learning because external pressures act to help an organization explore problems and prevent future failures (March 1991; Ocasio 1997). On the other hand, Haunschild and Rhee (2004) investigated the effects of voluntary and involuntary recalls on subsequent recall rates in the automotive industry and demonstrated that voluntary recalls result in more learning than involuntary recalls. They argued that involuntary recalls result in shallower learning processes, and concluded that organizational volition is important for learning because

autonomy increases commitment and problem analyses, whereas external pressures likely lead to defensive reactions that are not coupled to the organization in any useful way.

Researchers have further begun to explore the impact of organizational learning on the relationship between security investment and security performance (Cavusoglu et al. 2008; Herath and Herath 2008; Puhakainen and Siponen 2010). Note that investments in new security controls include the learning required for deployment. While the security investment literature has studied the impact of organizational learning on investment decisions or resource allocation, our study focuses on the impact of antecedent factors (i.e., security failures or external mandates) on organizational learning and ultimately security performance. We categorize security investments as proactive if they occur before any incident and reactive if they occur after an incident (with or without external regulatory pressure). Given that proactive and reactive investments both lead to organizational learning through security resource allocation/deployment, the differential effects between proactive and reactive investments likely resides in the difference between their learning effects during the resource allocation/deployment process. This observation motivated us to investigate whether proactive or reactive investments related to security breach incidents have any difference on security improvement as well as how external regulatory pressures affect security performance. Answering these questions will help policy makers and researchers understand the potential impact of new regulation and the value of carrot (investment incentives) vs. stick (breach reporting) policies.

Further, we consider the impact of information sharing among organizations and the economic incentive mechanisms for information security as a public good (Gal-Or and Ghose 2005). In the healthcare sector, organizations often share patient information as patients move between local clinics, small hospitals, tertiary care centers, and long-term rehabilitation centers. Likewise

information is often shared between clinics and outsourced providers such as laboratories. Security investments at any point in the healthcare system benefit all players (Appari and Johnson 2010). The public-good nature of information security within healthcare makes it possible to study the social learning effects stemming from security investments. Moreover, HIPAA addresses the interchange of information between organizations by mandating that organizations comply with privacy and security standards. Thus, regulatory pressure is relevant at both the individual organization level and for groups of organizations.

This study contributes to the literature on security investments and organizational learning theory in several ways. First, it provides a deeper understanding of the effects of security investments on subsequent performance, based on well-established learning theory. Second, it identifies the impacts of government regulation and an organization's proactive security investments. Lastly, it extends the scope of the learning analysis from an individual organization level to a regional level (in our case, the U.S. state level). We do so by examining the shared benefit of individual hospital investment for all hospitals within the same state.

The paper is organized as follows: The next two sections propose relevant research hypotheses based on organizational learning theory and describe the research methodology and data collection. Then the results are presented in section four. Finally, in the last section, implications and conclusions are discussed.

Hypotheses Development

From an economic perspective, an investment refers to the purchase of durable equipment, software, processes, knowledge, etc., in anticipation of future favorable returns on that investment (ROI) (Teisberg 1994; Van Mieghem 1998). Some organizational scholars have viewed investment as the quest for improvement in the learning processes for problem-solving heuristics

and techniques (Hauser and Clausing 1988; Winter 1994). In the context of security, measuring ROI has proved particularly challenging because the success of such investment is “nothing happened” (Anderson 2001; Behara et al. 2006; Gordon and Loeb 2002). Thus, the organizational learning perspective is particularly useful in explaining the effects of security investments.

Organizational learning from investments for problem solving enables people and their organizations to explore root causes of problems and discover potential opportunities for shaping a better future (Mukherjee et al. 1998). Attewell (1992) argued that the investment in advanced technologies should be considered as a special category of innovative actions because of the burden of organizational learning they impose on employees. Ittner et al. (2001) categorized investments into proactive and reactive approaches, assuming that both have a positive impact, but with different effects on organizational performance. The proactive approach argues that organizational learning occurs as a result of an organization’s (proactive) innovative actions (Fine 1986; Li and Rajagopalan 1998). Reactive investments are triggered by failures that require remedial action (Marcellus and Dada 1991).

Consistent with these arguments, organizational learning also influences the link between security investment and security performance because many employees in an organization, not just the security department, must be involved in learning the new systems and security controls. The know-how and technical knowledge associated with such IT security controls will be created by employees via the process of learning by doing (Attewell 1992), which occurs for both proactive and reactive investments. Thus both proactive and reactive investments result in organizational learning, implying the following hypotheses.

HYPOTHESIS 1. *Proactive security investments will result in the reduction of subsequent security failures.*

HYPOTHESIS 2. *Reactive security investments will result in the reduction of subsequent security failures.*

While testing for the association between security investment and security performance will help us better understand investment effectiveness, it is also meaningful to investigate the differences between these two types of investments (it can help illuminate the antecedent factor of an investment). Since proactive investment has no prior information about critical or weak points in an organization, it requires a clear understanding and analysis of security vantage points (definition and vision), government and public expectations, perceived security concerns, and determinants of security. Thus, in general, proactive investment is deployed by the waterfall approach (Frakes and Kang 2005). First, the target domain (i.e., security) is analyzed, and then controls for the domain are defined and implemented considering foreseeable variations. Therefore, proactive approaches lie at the heart of an organization's strategy to gain competitive advantage. However, this approach tends to require a large upfront investment—particularly with security because the threat models are constantly evolving, making it difficult to prepare for every possible failure.

Hence, rather than overinvest proactively, some organizations wait to observe attacks and use this knowledge to better allocate security spending (Bohme and Moore 2010). A reactive strategy implies that an organization is responding to experience so that the failures can be addressed efficiently and effectively. Bohme and Moore (2010) suggest that increasing uncertainty about the weakest links in information security makes it difficult for the organization to know which assets to protect. That uncertainty can lead to the organization to decide against security investments until a failures or weak point is realized. Thus, uncertainty leads to reactive investments. In fact, in cases with high uncertainly, it may to be rational to underinvest in security. Reactive investments focus on cost-effectiveness, rather than performance-effectiveness as a major source of

differentiation or competitive advantage (Ittner et al. 2001; Shankar 2006). Of course, recovering from repeated failures does not lead to customer satisfaction; however, recovery from a few failures through rapid remedial action typically avoids significant dissatisfaction and in some cases can build customer confidence (Karande et al. 2007).

Healthcare is generally less sophisticated and lags in adoption of the latest security technologies, as compared with industries like financial services. This observation supports the conclusion that uncertainty over the weakest links in healthcare may be lower than in industries with a long history of cyber-attack (like financial service). Lower uncertainty means that healthcare organizations often have not yet addressed known vulnerabilities that represent a weak link. Such a situation favors proactive security investment. Given a similar level of low uncertainty about the weakest links (low hanging fruit) across the healthcare sector, we hypothesize that the effect of proactive investments (and the learning required to understand the uncertainties) should be larger than that of reactive investments.

HYPOTHESIS 3. The effect of proactive security investments on the reduction of subsequent security failures is larger than that of reactive security investments.

It is also important to consider the impact of external mandates like government requirements on investment decisions. Understanding organizational responses to external regulatory pressure has implications for policy decisions within information security. Previous literature from various disciplines has investigated organizational responses to government-mandated changes (Majumdar and Marcus 2001; Marcus 1988; Saari et al. 1993). Commonly, they have considered government requirements as the activation of attention that can make organizations focus on a problem area. Since government requirements addressing a failure tend to be well-publicized pressures,

organizations may be forced to learn more from these pressures—thus overcoming inertia and stimulating organizational change (Ocasio 1997). March (1991) argues that organizations are apt to engage in exploitation of well-known practices, rather than explore of new ones. This supports the idea that external pressures can stimulate organizational learning and change. Such external pressures promote learning because they cause organizational members to pay more attention to failures, exploit them more deeply, and work to prevent them in the future.

Over the last decade, breach notification laws have required organizations to notify the information owners of security breaches. Breach notification laws create significant organizational pressure, both because of the cost of notification and because of likely negative press coverage. The attention-getting aspects of breach notifications help overcome organizational inertia and initiate learning by doing by taking actions to improve information security. Accordingly, such pressure is likely to draw organizational attention to security breaches and result in new organizational processes aimed at reducing future failures. This leads to the following hypothesis.

HYPOTHESIS 4. External pressure will result in the reduction of subsequent security failures.

In addition to the independent effects of external pressures and investments (both proactive and reactive), there are likely to be interaction effects as well: in particular, interaction between the learning effects of external pressures and investments. For example government regulations, like breach notification laws, require providers and payers in the healthcare sector to take specific actions with real costs to the organization. While specific guidelines decrease a level of uncertainty in certain weak points, passive focus on these points may cause the organization to ignore the broader understanding of security that is required for a proactive approach. Thus, the attention activated by a government requirement can make organizations simply focus on the indicated

layers (Radner and Rothschild 1975; Winter 1981) rather than assess security at all operational layers.

Some researchers have argued that reactive investments are generally targeted towards common failures and thus the information provided by a government requirement might extend the range of reactive investments or force the organizations to address them more deeply (Rowe and Gallaher 2006; Zollo and Winter 2002). Even so, other researchers have argued that such mandated procedures are unlikely to result in the type of deep learning required to enable the detection and correction of future failures (Bowie and Jamal 2006). With this mixed theoretical support, we do not have a clear basis for the direction of the regulatory impact. Thus in our current study, we simply test how mandated procedures influence proactive and reactive investments and subsequently security performance (without hypothesizing a positive or negative affect). We hypothesize that:

HYPOTHESIS 5. External pressure influences the effect of proactive security investments on the reduction of subsequent security failures.

HYPOTHESIS 6. External pressure influences the effect of reactive security investments on the reduction of subsequent security failures.

Research Methodology

Figure 1 illustrates our research model and hypotheses discussed in the prior section. We test the hypotheses using a Cox proportional hazard model.

The Cox Proportional Hazard Model

Our data on security failures and security investment within healthcare organizations includes breach timing and the adoption timing of security controls. This allows us to employ a statistical

method that considers the dependence of the organization's security *survival* or *failure* on the explanatory variables. Hazard functions are particularly useful for such analysis examining the impact of explanatory variables on the timing or probabilities of failure at an organization level (Eliashberg et al. 1997; Kauffman et al. 2000; Li et al. 2010). For example, Eliashberg et al. (1997) employed a proportional hazard model to assess the size of a reserve needed by a manufacturer to meet future warranty claims. Kauffman et al. (2000) adopted a hazard model to test for a market-wide network externality effect on network adoption. Li et al. (2010) used the Cox model to relate software firms' capabilities to their failure rates. These studies analyzed "time to events" and explored the effects of a variety of explanatory variables.

Among hazard models, the Cox model includes other attractive features. The model does not depend on distributional assumptions of survival time; provides flexibility for time dependent explanatory variables; and allows the hazard ratio to be defined as the relative risk based on a comparison of event rates. In particular, information security requires large capital expenditures and significant ongoing maintenance costs, because security features quickly grow obsolete as needs evolve with changing attacker strategies. Therefore, we employ the Cox model to examine the relative association between the effects of explanatory variables (i.e., security investment and regulatory requirement) and subsequent security failures.

Research Model

The hazard function, $h(t)$, refers to the failure rate of a subject per unit of time (t). The model assumes that the elapsed time to fail, T , is conditional on the explanatory variables. In our study, T measures the time from investment until either the event of interest – security failure – occurs or the end of the observation period. Thus, our hazard ratio represents the relative risk of security failures within a time unit (where the time unit is one month). The Cox model is expressed as:

$$h_i(t) = h_0(t) e^{\sum_{j=1}^K \beta_j x_{ij}} \quad \text{Eq.(1)}$$

where β_j is a vector of unknown regression parameters to be estimated for $j=1, \dots, K$. The baseline hazard function $h_0(t)$ corresponds to the case where $x_j=0$, involving time but not explanatory variables. The second component is the exponential functions with the sum of $\beta_j x_{ij}$, which involves explanatory variables but not time at an organization i . The model is referred to as a semi-parametric model since one part of the model involves the unspecified baseline function over time and the other part involves a finite number of regression parameters (Cox 1972). The semi-parametric Cox model is flexible and robust because it does not require assumptions about the baseline distribution.

The hazard ratio, or relative hazard, indicates the expected change in the risk of the terminal event when x changes from zero to one. If the hazard ratio is one, x has no effect. If the hazard ratio is greater than one, x is associated with increased survival, and vice versa.

$$\frac{h_i(t)}{h_0(t)} = e^{\sum_{j=1}^K \beta_j x_{ij}} \quad \text{Eq.(2)}$$

Cox regression coefficients β_j are estimated by partial likelihood (L), which is determined by the product of individuals' failure risks at each time (t). The failure likelihood of each individual is the hazard ratio, $h_i(t)$, of an individual (i) divided by the hazard, $h_i^c(t)$, of all the other organizations (R_i) (May et al. 2008).

$$\prod_{i=1}^N \frac{e^{(\beta_1 x_{1i} + \dots + \beta_k x_{ki})}}{\sum_{l \in R_i} e^{(\beta_1 x_{1l} + \dots + \beta_k x_{kl})}} = \prod_{i=1}^N \frac{h_i(t)}{h_i^c(t)} \quad \text{Eq.(3)}$$

Most commonly, this examination entails the specification of a linear-like model for the log hazard. The Cox model maximizes the log-likelihood function (LL) with respect to the parameters of interest, β_j .

$$LL(\beta) = \sum_{i=1}^N (h_i(t) - h_i^c(t)) = \sum_{i=1}^N \beta_i(x_i - x_i^c) = \beta_0 + \beta_1 \widehat{x}_{1i} + \dots + \beta_k \widehat{x}_{ki} \quad \text{Eq.(4)}$$

Generalizing the above equation, our Cox model examines the effects of security investment and regulatory requirements on the time until security failures.

Endogeneity of Security Investments

It is well known that organizational strategy self-selection complicates the empirical estimation of strategy performance, since an organization's propensity to make strategic decisions may be endogenously determined (Greene 1981; Li and Hitt 2008; Susarla and Barua 2011). Failing to account for endogeneity in organizational performance could lead to potentially misspecified and biased results (Greene 2003). In our study, there may be differences between the organizations who proactively invested and those who did not. For instance, those who proactively invested might have better senior management, resources, or technological expertise than those who did not. While the use of instrumental variables is one approach to account for endogeneity, an alternative approach to control for potential self-selection bias is to use a two-step econometric procedure proposed by Heckman (1979). Shaver (1998) extended the Heckman correction and showed that accounting for strategy self-selection changes the interpretation of how entry mode choice affects a firm's direct investment survival, distinguishing between greenfield entry and entry via acquisition.

Following Shaver (1998), in the first stage we use probit regression to estimate the probability that an organization prevents any breach as a function of security investment, size, types, and revenue. Based upon the results of the probit model in the first-stage, we predicted and saved the value for the inverse Mill's ratio (λ_i), which is calculated as $\hat{\lambda}_i = \phi(\hat{y}_i\omega_i)/\Phi(\hat{y}_i\omega_i)$, where ϕ and Φ are, respectively, the probability density function and cumulative distribution function of the standard normal distribution. \hat{y}_i and ω_i are the vector of independent variables and coefficients from the first-stage probit model (Heckman 1979; Shaver 1998). Figure 2 describes the first-stage probit model with information breaches and security investments on the time line. The inverse of Mill's ratio is a function of the probability that an organization prevents a breach. In the second-stage, the Cox model includes the inverse of Mill's ratio as a control variable to estimate an organization's hazard rate with its different types of security investment and other explanatory variables (Billari and Liefbroer 2007; Bushway et al. 2007; Hoang and Rothaermel 2010; Spohn and Holleran 2002).

While the analysis was conducted with total investment in Model (1), we also separately ran the model with proactive and reactive investment in Models (2) and (3). The general system-form of the models used to test the hypotheses is:

$$\begin{aligned}
 h_i(t)_{Total} &= h_0(t) \exp [\beta_1(Investment_i) + \beta_2(Proactive_i) + \beta_3(Law_i) \\
 &\quad + \beta_4(Law_i \times Proactive_i) + \beta_5(Law_i \times Investment_i) + \beta_\lambda \lambda_i \quad \text{Model (1)} \\
 &\quad + \delta_1(size_i) + \delta_2(Performance_i) + \delta_3(Type_i) + \tau(Year_i)]
 \end{aligned}$$

$$\begin{aligned}
 h_i(t)_{Proactive} &= h_0(t) \exp [\beta_1(ProactiveInvestment_i) + \beta_3(Law_i) \\
 &\quad + \beta_5(Law_i \times ProactiveInvestment_i) + \beta_\lambda \lambda_i + \delta_1(size_i) \quad \text{Model (2)} \\
 &\quad + \delta_2(Performance_i) + \delta_3(Type_i) + \tau(Year_i)]
 \end{aligned}$$

$$\begin{aligned}
 h_i(t)_{Reactive} &= h_0(t) \exp [\beta_1(ReactiveInvestment_i) + \beta_3(Law_i) \\
 &\quad + \beta_5(Law_i \times ReactiveInvestment_i) + \beta_\lambda \lambda_i + \delta_1(size_i) \quad \text{Model (3)} \\
 &\quad + \delta_2(Performance_i) + \delta_3(Type_i) + \tau(Year_i)]
 \end{aligned}$$

Empirical Analysis

Data Sources and Samples

We employed data from the Healthcare Information and Management Systems Society (HIMSS) Analytics™ Database⁴ from 2005 to 2009. During this period, HIMSS used a consistent database structure. The database provides information about the adoption of health information technologies – EMR and security applications – in healthcare organizations. It also includes various descriptive variables, which can serve as control variables such as the size of a healthcare organization, location, academic status, and so on. These data have been widely used in previous studies to examine the impact of healthcare information systems (Angst and Agarwal 2009; Hillestad et al. 2005; Miller and Tucker 2009). For the period 2005-2009, we initially gathered data on 4,487 organizations. Among them, 2,101 were dropped because of missing data, and thus our final sample includes 2,386 organizations. To determine whether our sample is representative of all organizations in the healthcare industry, we compared the sample with all organizations on several measures (the bed size, IT equipment, security investment, and performance) by conducting two-sample *t*-tests. The *t*-tests indicated that all *p*-values are larger than 10% as seen in Table 1. Thus, we cannot reject the null hypothesis that the two sample means are the same on each measure and conclude that the healthcare organizations in our study are representative of the healthcare industry.

Next, we matched the sample data with 281 reported healthcare security breaches from January 2005 to June 2010. We employed three sources to obtain information breaches: Health & Human Services (HHS)⁵, Identity Theft Resource Center (ITRC)⁶, and Data Loss Database⁷.

⁴ See http://www.himss.org/foundation/histdata_about.asp, It integrated healthcare delivery networks and provides their detailed historical data about information technology (IT) use.

⁵ See <http://www.hhs.gov/>, As required by the HITECH Act, HHS posts a list of breaches of unsecured protected health information affecting 500 or more individuals.

Measurement of Variables

Security failure is our primary outcome and is measured using a binary variable: 1, if the organization had breach in that time period, 0 otherwise. The *survival time* is modeled as the length of time or duration that an organization remains without any breach (in months). For *security investment*, we counted the number of IT security controls that were adopted. HIMSS provides data on the adoption of anti-virus, encryption, firewall, intrusion detection, user authentication, and spam filter.

We classified the security investment decisions into two types: *proactive vs. reactive*. Healthcare organizations are often affiliated with a group that consists of a main organization named as *parent* and other sub-organizations affiliated to the “*parent*”. Given this structure, if an organization invested in an IT security control within one year after any member of its group experienced a breach, we say that is a reactive investment (and thus *proactive* has a value of 0; otherwise 1). In addition, we also distinguish whether post-incident investments were reactions to breaches or were already planned prior to breaches. The HIMSS database indicates whether the adoption of a certain IT security control is planned for a specific year. If an organization planned an investment in year $t-1$ and made a reactive investment in year t , the investment was not coded as a reactive investment.

We also incorporated state security breach notification laws (*Law*) into our model in order to investigate the effect of regulatory requirements on security performance. Data on state legislation

⁶ See <http://www.idtheftcenter.org/>, *The ITRC breach list is a compilation of data breaches confirmed by various media sources and/or notification lists from state governmental agencies.*

⁷ See <http://datalossdb.org>, *The database is a collection of breach notification letters sent to various jurisdictions in the United States. These were gathered by staff and volunteers through sponsorship funding and donations.*

over the observation period were collected from the National Conference of State Legislatures (NCSL)⁸.

For further investigation of the effects of security failures, we employed two different variables to distinguish the types of security breaches. First, *Inside*: breaches from inside an organization include lost-devices or accidentally exposed healthcare information cases, as well as malicious insider activity. Second, *Outside*: breaches from outside an organization are those committed by outsiders' unauthorized access, such as hacking or stolen devices. The distinction is often important in that the perceived risks related to misuse of breached information is different.

Control variables in the analysis include *bed size*, *academic*, *hospital*, *IT equipment*, *performance*, and *calendar year*. *Bed size* is the number of licensed beds, which has been widely used to represent a healthcare organization's size and available resources. *Academic* and *hospital* are dummy variables to describe organization type. If an organization includes an academic institute, *academic* was set to 1; otherwise 0. *Hospital* was set to 1 if the organization is an acute care hospital, while 0 includes all the other types such as sub-acute, ambulatory, and integrated delivery systems (IDS). *IT equipment* is the number of computer/laptops operated over that period. *Organization performance* is the net income that a system generated from patient care, investments and other sources in that time period (revenues in excess of expenses). The *years* between 2005 and 2010 were coded as dummy variables, which have value of 1 if the data are for a particular year and 0 if not. The base year in our analysis is 2005. Table 2 provides descriptive statistics for the variables in our analysis.

⁸ See <http://www.ncsl.org/>, NCSL provides access to current state and federal legislation and a comprehensive list of state documents including state statutes, constitutions, legislative audits and research reports.

Results

First, we assessed the correlations between the explanatory variables of the Cox model. Table 3 displays the correlation matrix with the tolerance values and the variance inflations (VIFs). Most of the correlations among the variables show low values, and multicollinearity diagnostics exhibit tolerance values between 0.42 and 0.99, which are above the common cutoff threshold of 0.1 (Hair et al. 2005). The variance inflations (VIFs) of all variables are less than 2.38. A usual threshold of VIFs is 10.0, which corresponds to a tolerance of 0.1. Therefore, the multicollinearity is not a concern for our models.

To test the hypotheses, we ran the Cox model to evaluate organization-specific variables as determinants of subsequent security failure. The analyses were performed by Models (1), (2), and (3) on the two levels: an organization level and a state level. While Model (1) tests the effect of total security investments across all our analyses, Models (2) and (3) investigate the effects of proactive and reactive security investments, respectively.

Table 4 and 5 present the estimates of the parameters (β_i) and hazard rates ($h(t)$) for the models. H1 and H2 argue that proactive and reactive security investments reduce the subsequent security failures of an investing organization. As shown in Table 4, when we first tested the total investment in Model (1), the investment decreases the subsequent security failures ($\beta_I = -0.279$ at $p < 0.01$) with a hazard rate ($h(t) = 0.757$). Next, we separately examined proactive and reactive investments. The estimation yielded by Model (2) supports H1 with a negative coefficient ($\beta_I = -0.653$ at $p < 0.01$) for proactive investments, but Model (3) does not support H2. Note that proactive investment has a hazard rate of 0.52 (less than one). This observation implies that proactive investments reduce the likelihood of a security failure by about 48%, while reactive investments do not have any significant effect on security failures.

To further investigate the social effects from security investments, we ran the three models at a state level. As Table 5 displays, the state-level analysis supports both H1 and H2 with $\beta_I = -1.426$ at $p < 0.01$ ($h(t) = 0.240$) and $\beta_I = -0.902$ at $p < 0.01$ ($h(t) = 0.406$), respectively. While reactive investments do not have any significance at an organization level, they significantly reduce subsequent security failures at a state level. Comparing the coefficients suggests that proactive investments reduce subsequent security failures more than reactive investments at both levels. In addition, the magnitude of proactive investments becomes larger at the state level than the organization level (76% vs. 48% in reduction). The effect of total investments results in less security failures at the state level ($\beta_I = -1.545$ at $p < 0.01$) than the organization level ($\beta_I = -0.279$ at $p < 0.01$).

Figure 3 describes the differences of the hazard rates between the organization and a state level. The graph shows that the hazard rates of both proactive and reactive investments are lower at the state level than at the organization level. The difference between proactive and reactive investments decreases at the state level. These results are consistent with both the theories of organizational learning and public goods.

We next statistically compared the effect of proactive investments to that of reactive investments on subsequent security failures (Hypothesis 3). The above tests, where proactive and reactive investments were examined as separate variables for Hypothesis 1 and 2, already demonstrated proactive investment has larger negative effect (coefficient) and smaller hazard rate than reactive investment at both levels. It is not uncommon for researchers to separately compare the effects of different types on a focal variable. However, a simple comparison using separate variables is not completely satisfying, because we cannot perform a formal statistical test of the difference between the coefficients. Even though the coefficients are (individually) statistically

significant, the differences between them may not be significant. For this comparison, a formal statistical analysis through an indicator is preferable because it provides a means of formally testing the difference between the coefficients (Jaccard 2001). Therefore, Model (1) includes an indicator ($Proactive_i$), which represents proactive investments, to test the Hypothesis 3. The coefficient of proactive type is -1.011 ($p < 0.01$) at the organization level, and is -2.561 ($p < 0.01$) at the state level. Although the coefficients are negative at both organizational and state levels, the magnitude is larger at the state level. This indicates that proactive investments result in lower failure rates than reactive investments at both levels and the impact of proactive investments is amplified at the state level. Therefore, we can conclude that fewer security failures occur when an organization proactively investments (as opposed to reactive investments) and the impact of the investments has been increased at an aggregate level due to information sharing and learning effects.

External pressure, like government regulations, is another important focal variable that affects organizational learning. H4 argues that an external pressure can reduce subsequent security failures. We tests H4 by investigating how the existence of breach notification laws affects subsequent security failures in a state. We find full support for this hypothesis with Models (1), (2), and (3). Model (1) shows the coefficients of the laws, -1.067 ($p < 0.01$, $h(t)=0.344$) at the organization level, and -1.722 ($p < 0.01$, $h(t)=0.179$) at the state level. Likewise, Models (2) and (3) have -0.888 ($p < 0.01$, $h(t)=0.411$) and -1.016 ($p < 0.01$, $h(t)=0.362$) at the organization level, and -1.238 ($p < 0.01$, $h(t)=0.290$) and -1.363 ($p < 0.01$, $h(t)=0.256$) at the state level. Our models consistently indicate that externally mandated procedures are associated with improved security performance. Further, an external pressure has a larger effect at the aggregate level.

Lastly, in order to test Hypothesis 5 and 6, we examine the interaction effects of an external pressure and proactive/reactive investments through the addition of product terms. At the organization level, external regulatory pressure significantly attenuates the effects of proactive investments on subsequent security failures with a positive coefficient, 0.237 ($p < 0.01$, $h(t) = 1.267$). However, it does not significantly affect the effect of reactive investment. Similarly, at the state level, external regulatory pressure also significantly influences the effect of proactive investments ($\beta_5 = 0.347$ at $p < 0.01$), but not on that of reactive investments ($\beta_5 = 0.024$ at $p < 0.05$).

Internal vs. External threats

Security breaches stem from both internal failures, such as accidental disclosures or malicious insiders, and external threats, such as outsider thefts or attacks. An issue we have not addressed is the learning effects associated with specific types of security failures. Our analysis assumes that an organization's concern about security failure costs and its willingness to prevent failures are the same for insider and outsider threats. However, security researchers point out that organizations often focus on preventing external attacks rather than insider threats, even though insider threats can be equally harmful (Liu et al. 2009; McFadzean et al. 2007). It has been also emphasized that an organization's perception affects the actual learning and future performance (Hurley and Hult 1998; Ryu et al. 2005; Zakay et al. 2004). Thus, if the organization views outside threats as more critical than inside threats, it may pay more attention to outside threats and indeed learn to better protect against them.

To investigate this question, we divided security failure into two groups: inside and outside. Since larger concerns about a problem lead to greater effort to resolve the problem, we expect the learning effects of security investments to be more highly associated with the reduction of subsequent security failures from outside an organization than inside. As shown in Tables 6 and 7,

the results demonstrate this prediction. The breaches from outsiders show very similar significance patterns with the overall breaches, whereas the breaches from insiders have no significant association with the explanatory variables. The failure in preventing external threats has significant negative associations with proactive investments (-0.734 at $p < 0.01$ and -0.988 at $p < 0.01$) at the organization and the state level. On the other hand, reactive investments are only significantly associated (negative) with external threats at the state level with -0.452 at $p < 0.01$. External pressure is negatively associated with breaches from outsiders at both levels (-1.041 and -2.334 at $p < 0.01$); however it weakens the effect of proactive investments (0.371 and 0.350 at $p < 0.01$). All of the main effects with external threats show positive social effects on security performance at the state level.

Endogeneity of Laws

Breach notification laws represent another endogeneity issue since regulation might be systematically enacted in states with higher breach incidents. Romanosky et al. (2011) raised the issue of endogenous adoption of breach notification laws and tested whether laws were adopted due to a sudden rise in identity theft. If laws were endogenous, we would expect to see that states would have an increased identity theft rate immediately before the adoption of legislation. Romanosky et al. (2011) demonstrated there has been no such systematic increase for states that adopted a breach disclosure law.

In the healthcare context, we examined the difference between the number of breaches in states immediately before the adoption of legislation and those of states without such laws by conducting two-sample t -test (at the state level). The t -test shows a p -value of 0.23. Thus, we conclude that the two sample means of the number of breaches with and without the adoption of legislation are not different, and the endogeneity of breach notification laws is not a concern.

Implications and Conclusions

Organizational learning is believed to be driven by a combination of investments and external pressures (Ittner et al. 2001; Li and Rajagopalan 1998). This study provides empirical tests of the hypotheses generated by considering the learning effects of proactive and reactive security investment with external pressure. The results indicate that proactive investments are more effective at reducing security failures than reactive investments. However, when proactive investments were forced by an external requirement, the effect of proactive investment was diminished. This implies that voluntary, proactive investments have the best performance. The findings have important implications for both security managers and policy makers. The importance of strategic (i.e., proactive and reactive) and regulatory factors in decisions on security investments suggests that security managers and a government should pay considerable attention to decision processes in security investments in order to maximize the learning effect of the investments.

We also find that the learning effects vary for different types of security failures. Organizations have different perceptions of security failures, and those threats that are perceived as more significant enhance the learning effects of security investment focused in that area. The implication is that organizations may be more concerned about external threats and thus may focus more investments on IT security to curb outsider threats rather than insider threats (Liu et al. 2009; Liza 2010). We note, however, that our investment data focuses on security controls and that preventing accidental or malicious inside threats also depends on education and internal policies.

Considering the social effects of organizational learning, the effects of both security investments and external pressures have larger magnitudes at an aggregate level than at an organization level. Security investments induce learning by doing or learning through

implementing controls, which typically involve many employees in the learning process. Government requirements also make an organization focus attention, which results in learning within problem areas. We infer that the organizational learning through the investments and government requirements create positive externalities—that one organization's security investments and regulatory compliance help the others' security.

Our results have implications for managers and researchers. They imply that it is important to understand which types of security investments provide the greatest learning benefits. Such learning is particularly important for organizations to maximize the effects of security investments under constrained resources and evolving security threats. Based on these results, we advise chief information security officers to place greater emphasis on proactive initiatives rather than maintain a purely reactive posture. Since attackers' abilities and resulting threats evolve quickly, learning from proactive initiatives rather than past failures is particularly important. Policy makers should consider regulation that combines proactive initiatives and external pressures—for example, mandating that a portion of the overall IT budget be dedicated to security while allowing the organizations to decide on the types of security investment. Alternatively, financial incentives like those in the HITECH legislation could be earmarked specifically for security. We note that while our analysis focuses on the healthcare sector, we believe that our findings can likely be generalized to other industries facing similar information risks.

Some important issues remain for future research. First, we considered only the adoption of IT security controls without addressing the issue of policies and training programs. While implementing controls such as training would have a direct learning effect, our study mainly focuses on indirect learning effects through learning by doing or learning by using IT security controls. Second, our model measures security investments as the number of IT security controls,

and not the momentary amount of the security investment. This study also does not consider the cost of a breach, viewing all publically reported breaches as equally bad. Future research could also consider longer periods. With the Cox model, it is common to observe that some organizations never experience an event within the study period. Data covering longer periods could help mitigate this limitation.

References

- Anderson, R. 1996. "A Security Policy Model for Clinical Information Systems." in *IEEE Symposium on Security and Privacy*, May, pp. 30-43.
- Anderson, R. 2001. "Why Information Security is Hard - An Economic Perspective," in *17th Annual Computer Security Applications Conference*, December, pp. 358-365.
- Angst, C.M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.
- Appari, A., and Johnson, M. E. 2009. "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management* (6: 4), pp. 279-314.
- Attewell, P. 1992. "Technology Diffusion and Organizational Learning - The Case of Business Computing," *Organization Science* (3:1), February, pp. 1-19.
- Behara, R., Derric, C., and Hu, Q. 2006. "A Process Approach to Information Security: Lessons from Quality Management," in *Americas Conference on Information Systems (AMCIS)*, Paper 169.
- Billari, F.C., and Liefbroer, A.C. 2007. "Should I stay or should I go? The Impact of Age Norms on Leaving Home," *Demography* (44:1), February, pp. 181-198.
- Bohme, R., and Moore, T. 2010. "The Iterated Weakest Link," *IEEE Security & Privacy* (8:1), January, pp. 53-55.
- Bowie, N.E., and Jamal, K. 2006. "Privacy Rights on the Internet: Self-regulation or Government Regulation?," *Business Ethics Quarterly* (16:3), July, pp. 323-342.
- Bushway, S., Johnson, B.D., and Slocum, L.A. 2007. "Is the Magic still There? The Use of the Heckman Two-Step Correction for Selection Bias in Criminology," *Journal of Quantitative Criminology* (23:2), June, pp. 151-178.
- 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.
- Cox, D.R. 1972. "Regression Models and Life-Tables," *Journal of the Royal Statistical Society Series B-Statistical Methodology* (34:2), pp. 187-220.
- Dorroh, J.R., Gulledge, T.R., and Womer, N.K. 1994. "Investment in Knowledge - A Generalization of Learning by Experience," *Management Science* (40:8), August, pp. 947-958.
- Eliashberg, J., Singpurwalla, N.D., and Wilson, S.P. 1997. "Calculating the Reserve for a Time and Usage Indexed Warranty," *Management Science* (43:7), July, pp. 966-975.

- Fine, C.H. 1986. "Quality Improvement and Learning in Productive Systems," *Management Science* (32:10), October, pp. 1301-1315.
- Frakes, W.B., and Kang, K. 2005. "Software Reuse Research: Status and Future," *IEEE Transactions on Software Engineering* (31:7), July, pp. 529-536.
- Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2), pp. 186-208.
- Gordon, L., and Loeb, M. 2002. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* (5:4), pp. 438-458.
- Gordon, L.A., and Loeb, M.P. 2006. "Budgeting Process for Information Security Expenditures," *Communications of the ACM* (49:1), January, pp. 121-125.
- Greene, W. H. 1981. "Sample Selection Bias as a Specification Error-Comment." *Econometrica* (49:3), pp. 795-798.
- Greene, W.H. 2003. *Econometric Analysis*, (5th ed.) Prentice Hall.
- Hair, J.F., Tatham, R.L., Anderson, R.E., and Black, W. 2005. *Multivariate Data Analysis* (6th ed.), Prentice Hall.
- Hatch, N.W., and Mowery, D.C. 1998. "Process Innovation and Learning by Doing in Semiconductor Manufacturing," *Management Science* (44:11), November, pp. 1461-1477.
- Haunschild, P.R., and Rhee, M. 2004. "The Role of Volition in Organizational Learning: The case of automotive product recalls," *Management Science* (50:11), pp. 1545-1560.
- Hauser, J.R., and Clausing, D. 1988. "The House of Quality," *Harvard Business Review* (66:3), pp. 63-73.
- Heckman, J.J. 1979. "Sample Selection Bias as a Specification Error," *Econometrica* (47:1), pp. 153-161.
- Herath, H.S.B., and Herath, T.C. 2008. "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit," *Journal of Management Information Systems* (25:3), pp. 337-375.
- Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., and Taylor, R. 2005. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs," *Health Affairs* (24:5), pp. 1103-1117.
- Hoang, H., and Rothaermel, F.T. 2010. "Leveraging Internal and External Experience: Exploration, Exploitation, and R&D Project Performance," *Strategic Management Journal* (31:7), July, pp. 734-758.
- Hurley, R.F., and Hult, G.T.M. 1998. "Innovation, Market Orientation, and Organizational Learning: An Integration and Empirical Examination," *Journal of Marketing* (62:3), July, pp. 42-54.
- Ittner, C.D., Nagar, V., and Rajan, M.V. 2001. "An Empirical Examination of Dynamic Quality-based Learning Models," *Management Science* (47:4), April, pp. 563-578.
- Jaccard, J. 2001. *Interaction effects in logistic regression*, A SAGE University Paper.
- Johnson, M.E. 2009. "Data Hemorrhages in the Health-Care Sector," *Financial Cryptography and Data Security* (5628:2009), pp. 71-89.
- Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce* (12:1), pp. 69-91.
- Karande, K., Magnini, V.P., and Tam, L. 2007. "Recovery Voice and Satisfaction After Service Failure: An Experimental Investigation of Mediating and Moderating Factors," *Journal of Service Research* (10:2), November, pp. 187-203.

- Kauffman, R.J., McAndrews, J., and Wang, Y.M. 2000. "Opening the "Black Box" of Network Externalities in Network Adoption," *Information Systems Research* (11:1), March, pp. 61-82.
- Kolfal, B., Patterson, R., and Yeo, L. 2010. "Market Impact on IT Security Spending," in *The Ninth Workshop on the Economics of Information Security*, Harvard University.
- Li, G., and Rajagopalan, S. 1998. "Process Improvement, Quality, and Learning Effects," *Management Science* (44:11), November, pp. 1517-1532.
- Li, S.L., Shang, J., and Slaughter, S.A. 2010. "Why Do Software Firms Fail? Capabilities, Competitive Actions, and Firm Survival in the Software Industry from 1995 to 2007," *Information Systems Research* (21:3), September, pp. 631-654.
- Liu, D.B., Wang, X.F., and Camp, L.J. 2009. "Mitigating Inadvertent Insider Threats with Incentives," in *Financial Cryptography and Data Security*, R. Dingledine and P. Golle (eds.), pp. 1-16.
- Li, X., and Hitt, L. M. 2008. "Self-Selection and Information Role of Online Product Reviews." *Information Systems Research* (19:4), pp. 456-474.
- Lohmeyer, D.F., McCrory, J., and Pogreb, S. 2002. "Managing information security," in *The McKinsey Quarterly*.
- Majumdar, S.K., and Marcus, A.A. 2001. "Rules versus Discretion: The Productivity Consequences of Flexible Regulation," *Academy of Management Journal* (44:1), February, pp. 170-179.
- Marcellus, R.L., and Dada, M. 1991. "Interactive Process Quality Improvement," *Management Science* (37:11), November, pp. 1365-1376.
- March, J.G. 1991. "Exploration and Exploitation in Organizational Learning," *Organization Science* (2:1), pp. 71-87.
- Marcus, A.A. 1998. "Implementing Externally Induced Innovations - a Comparison of Rule-Bound and Autonomous Approaches," *Academy of Management Journal* (31:2), June, pp. 235-256.
- Marcus, A.A., and Nichols, M.L. 1999. "On the Edge: Heeding the Warnings of Unusual Events," *Organization Science* (10:4), pp. 482-499.
- May, S., Hosmer, D.W., and Lemeshow, S. 2008. *Applied Survival Analysis: Regression Modeling of Time-to-Event Data / David W. Hosmer, Stanley Lemeshow, Susanne May* Wiley-Interscience, Hoboken, N.J.
- McFadzean, E., Ezingard, J.N., and Birchall, D. 2007. "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level," *Online Information Review* (31), pp. 622-660.
- Miller, A.R., and Tucker, C. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science* (55:7), pp. 1077-1093.
- Mukherjee, A.S., Lapre, M.A., and Van Wassenhove, L.N. 1998. "Knowledge Driven Quality Improvement," *Management Science* (44:11), November, pp. 35-49.
- Mulligan, D.K., and Bamberger, K.A. 2007. "Security Breach Notification Laws: Views from Chief Security Officers," University of California-Berkeley School of Law.
- Naveh, E., and Marcus, A.A. 2004. "When does the ISO 9000 Quality Assurance Standard Lead to Performance Improvement? Assimilation and going beyond," *IEEE Transactions on Engineering Management* (51:3), August, pp. 352-363.
- Ocasio, W. 1997. "Towards an Attention-Based View of the Firm," *Strategic Management Journal* (18), pp. 187-206.

- Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), December, pp. 757-778.
- Radner, R., and Rothschild, M. 1975. "Allocation of Effort," *Journal of Economic Theory* (10:3), pp. 358-376.
- Roberds, W., and Schreft, S.L. 2009. "Data Breaches and Identity Theft," *Journal of Monetary Economics* (56:7), October, pp. 918-929.
- 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.
- Rowe, B.R., and Gallaher, M.P. 2006. "Private Sector Cyber Security Investment Strategies: An Empirical Analysis," in *The Eighth Workshop on the Economics of Information Security*, Cambridge, UK. Available: <http://weis2006.econinfosec.org/docs/18.pdf>.
- Ryu, C., Kim, Y.J., Chaudhury, A., and Rao, H.R. 2005. "Knowledge Acquisition via Three Learning Processes in Enterprise Information Portals: Learning-by-Investment, Learning-by-Doing, and Learning-from-Others," *MIS Quarterly* (29:2), June, pp. 245-278.
- Saari, J., Bedard, S., Dufort, V., Hryniewiecki, J., and Theriault, G. 1993. "How Companies Respond to New Safety Regulations - A Canadian Investigation," *International Labour Review* (132:1), pp. 65-74.
- Salomon, R., and Martin, X. 2008. "Learning, Knowledge Transfer, and Technology Implementation Performance: A Study of Time-to-Build in the Global Semiconductor Industry," *Management Science* (54:7), July, pp. 1266-1280.
- Shankar, V. 2006. "Proactive and Reactive Product Line Strategies: Asymmetries between Market Leaders and Followers," *Management Science* (52:2), February, pp. 276-292.
- Shaver, J.M. 1998. "Accounting for Endogeneity When Assessing Strategy Performance: Does Entry Mode Choice Affect FDI Survival?," *Management Science* (44:4), April, pp. 571-585.
- Spohn, C., and Holleran, D. 2002. "The Effect of Imprisonment on Recidivism Rates of Felony Offenders: A Focus on Drug Offenders," *Criminology* (40:2), May, pp. 329-357.
- Susarla, A., and Barua, A. 2011. "Contracting Efficiency and New Firm Survival in Markets Enabled by Information Technology." *Information Systems Research* (22:2), pp. 306-324.
- Teisberg, E.O. 1994. "An Option Valuation Analysis of Investment Choices by A Regulated Firm," *Management Science* (40:4), April, pp. 535-548.
- Van Mieghem, J.A. 1998. "Investment Strategies for Flexible Resources," *Management Science* (44:8), August, pp. 1071-1078.
- Wang, T.-W., Rees, J., and Kannan, K.N. 2008. "Reading the Disclosures with New Eyes: Bridging the Gap between Information Security Disclosures and Incidents," Working papers.
- Winter, S.G. 1981. "Attention Allocation and Input Proportions," *Journal of Economic Behavior & Organization* (2:1), pp. 31-46.
- Winter, S.G. 1994. *Organizing for continuous improvement: evolutionary theory meets the quality revolution* Oxford University Press, New York.
- Zakay, D., Ellis, S., and Shevsky, M. 2004. "Outcome Value and Early Warning Indications as Determinants of Willingness to Learn from Experience," *Experimental Psychology* (51:2), pp. 150-157.
- Zollo, M., and Winter, S.G. 2002. "Deliberate Learning and the Evolution of Dynamic Capabilities," *Organization Science* (13:3), pp. 339-351.

Table 1. Two sample *t*-test

Measure	<i>t</i> -value	<i>p</i> -value
security investment	-0.36	0.72
performance	-1.58	0.11
IT equipment	-0.72	0.47
bed size	-0.62	0.53

Table 2. Descriptive statistics for key variables

Variable (x_j)	Description	Mean	StdD	Min	Max
Security Failure	1 if a security breach occurs at year t , otherwise 0.	0.09	0.28	0.00	1.00
<i>Inside</i>	1 if an inside (malicious and accidental) beach occurs; otherwise 0	0.03	0.16	0.00	1.00
<i>Outside</i>	1 if an outside breach occurs; otherwise 0	0.06	0.24	0.00	1.00
Survival Time	The length of time (months) that an organization remains without any breach.	18.13	13.95	1.00	65.00
Security investment	The number of IT security controls implemented at different layers.	1.29	1.71	0.00	6.00
Proactive Investment	The number of security investments without a breach experience.	1.17	1.67	0.00	6.00
Reactive Investment	The number of security investments with a breach experience.	0.12	0.64	0.00	6.00
Proactive Type	1 if a security investment occurs without a breach experience, otherwise 0.	0.43	0.49	0.00	1.00
Law	1 if a state has breach notification laws, otherwise 0	0.89	0.30	0.00	1.00
Control variables					
IT equipment	Log (number of computers and laptops operated)	3.58	1.61	0.00	8.00
Performance	Log(Annual revenue)	19.77	1.92	14.52	24.01
Bed size	Log (number of beds)	5.04	1.01	1.79	7.47
Academic	1 if the organization is academic, otherwise 0	0.07	0.26	0.00	1.00
Hospital	1 if the organization is an acute-care hospital, otherwise 0	0.92	0.27	0.00	1.00
<i>years</i>	1 if it is a particular year between 2005 and 2010, otherwise 0	–	–	0.00	1.00

Table 3. Correlation matrix for independent variables of the hazard model

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	Tol	VIFs
(1) Security Investment	1							0.43	2.34
(2) Proactive	0.73*	1						0.42	2.38
(3) Law	-0.06*	-0.04*	1					0.99	1.01
(4) IT equipment	0.00	-0.03*	0.04*	1				0.53	1.87
(5) Performance	-0.05*	-0.19*	-0.01	0.25*	1			0.84	1.18
(6) Bed Size	0.01	-0.05*	0.03*	0.68*	0.32*	1		0.50	1.99
(7) Academic	0.01	-0.01*	0.02*	0.32*	0.07*	0.30*	1	0.87	1.14
(8) Hospital	0.09*	0.21*	0.04*	-0.05*	-0.38*	-0.08*	0.08*	0.95	1.05

Notes. *represent statistically significant correlation coefficients with $p < 0.05$

Table 4. Hazard model results (organization level)

	Model (1)		Model (2)		Model (3)		Hypotheses
	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	
Proactive Investment			-0.653*** (0.126)	0.521			H1:Supported
Reactive Investment					0.114 (0.086)	1.121	H2:Not supported
Total Investment	-0.279*** (0.082)	0.757					
Proactive	-1.011*** (0.293)	0.364					H3:Supported
Law	-1.067*** (0.262)	0.344	-0.888*** (0.249)	0.411	-1.016*** (0.243)	0.362	H4:Supported
Proactive x Law	0.353 (0.345)	1.424					
SI x Law	0.158** (0.088)	1.171					
PI x Law			0.237* (0.144)	1.267			H5:Supported
Rlx Law					-0.064 (0.097)	0.938	H6:Not supported
Controls							
Inverse Mills ratio	-4.783** (2.410)	0.008	-4.401* (2.407)	0.012	-1.278 (2.280)	0.279	
IT equipment	0.192*** (0.057)	1.212	0.154** (0.056)	1.167	0.104** (0.054)	1.110	
Performance	-0.079* (0.049)	0.923	-0.064 (0.049)	0.938	-0.111** (0.048)	0.895	
Bed size	-0.084 (0.070)	0.919	-0.056 (0.068)	0.945	-0.085 (0.069)	0.918	
Academic	1.683*** (0.347)	5.383	1.691*** (0.349)	5.424	1.356*** (0.327)	3.880	
Hospital	-5.043*** (0.330)	0.006	-4.928*** (0.333)	0.007	-4.859*** (0.317)	0.008	
2006	0.165 (0.304)	1.179	0.688** (0.278)	1.990	0.606** (0.304)	1.833	
2007	-0.735** (0.299)	0.480	-0.297 (0.272)	0.743	-0.197 (0.293)	0.821	
2008	-0.859** (0.324)	0.423	-0.436 (0.295)	0.646	-0.346 (0.320)	0.708	
2009	-3.195*** (0.359)	0.041	-2.786*** (0.324)	0.062	-2.224*** (0.345)	0.108	
2010	-3.128*** (0.323)	0.044	-2.720*** (0.287)	0.066	-2.382*** (0.312)	0.092	
LL ⁺	-2684.95		-2671.84		-2715.38		

Notes. Standard errors are in parentheses. *p*-values are represented by * Significant at $p < 0.1$, ** Significant at $p < 0.05$, *** Significant at < 0.01

*Hazard models are estimated using log likelihood(LL) functions and LL indicates the fit of the model with higher values indicating a better fit.

Table 5. Hazard model results (state level)

	Model (1)		Model (2)		Model (3)		Hypotheses
	β_i	$h(t)$	β_i	$h(t)$	β_i	$h(t)$	
Proactive Investment			-1.426*** (0.233)	0.240			H1:Supported
Reactive Investment					-0.902*** (0.199)	0.406	H2:Supported
Total Investment	-1.545*** (0.216)	0.213					
Proactive	-2.561*** (0.432)	0.077					H3:Supported
Law	-1.722*** (0.365)	0.179	-1.238** (0.320)	0.290	-1.363*** (0.301)	0.256	H4:Supported
Proactive x Law	1.630*** (0.449)	5.101					
SI x Law	0.224*** (0.056)	1.251					
PI x Law			0.347** (0.153)	1.414			H5:Supported
RIx Law					0.024 (0.034)	1.024	H6:Not Supported
Controls							
Inverse Mills ratio	-2.860* (1.571)	0.057	-1.097 (1.438)	0.334	-0.692 (1.448)	0.501	
IT equipment	0.033*** (0.006)	1.034	0.027** (0.005)	1.028	0.016** (0.005)	1.016	
Performance	0.036*** (0.006)	1.037	-0.002 (0.003)	0.998	-0.005*** (0.002)	0.995	
Bed size	0.066*** (0.020)	1.068	-0.006 (0.010)	0.994	-0.033*** (0.009)	0.967	
Academic	1.706*** (0.222)	5.506	1.208*** (0.202)	3.347	1.261*** (0.205)	3.530	
Hospital	-5.397*** (0.384)	0.005	-4.429*** (0.313)	0.012	-4.529*** (0.312)	0.011	
2006	-0.015 (0.479)	0.986	-0.000 (0.478)	1.000	-0.010 (0.473)	0.989	
2007	-0.926* (0.441)	0.396	-0.835** (0.440)	0.743	-0.872** (0.437)	0.418	
2008	-1.876*** (0.473)	0.153	-1.724*** (0.473)	0.646	-1.722*** (0.472)	0.179	
2009	-2.683*** (0.486)	0.068	-2.261*** (0.488)	0.062	-2.202*** (0.485)	0.111	
2010	-2.369*** (0.449)	0.094	-2.149*** (0.447)	0.066	-2.179*** (0.446)	0.113	
LL ⁺	-1991.07		-2027.39		-2033.77		

Notes. Standard errors are in parentheses. *p*-values are represented by * Significant at $p < 0.1$, ** Significant at $p < 0.05$, *** Significant at < 0.01

*Hazard models are estimated using log likelihood(LL) functions and LL indicates the fit of the model with higher values indicating a better fit.

Table 6. Hazard model results by breach type (organization level)

	Inside						Outside					
	Model (1)		Model (2)		Model(3)		Model (1)		Model (2)		Model(3)	
	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$
Proactive Investment			-14.613 (690)	0.000					-0.734*** (0.124)	0.480		
Reactive Investment					-11.488 (699)	0.000					0.057 (0.086)	1.059
Security Investment	-12.247 (645)	0.000					-0.287*** (0.078)	0.751				
Proactive Law	-3.776 (1705)	0.023					-1.140*** (0.299)	0.320				
Law	0.392 (1.372)	1.480	-0.532 (1.174)	0.587	0.827 (1.183)	2.286	-1.041*** (0.245)	0.353	-0.764*** (0.231)	0.466	-0.684*** (0.215)	0.505
Proactive x Law	9.363 (1705)	>1000					0.400 (0.355)	1.491				
SI x Law	11.805 (645)	>1000					0.248 (0.080)	1.282				
PI x Law			14.135 (690)	>1000					0.371*** (0.140)	1.450		
RIx Law					10.725 (699)	>1000					0.098 (0.093)	1.104
Controls												
Inverse Mills ratio	-18.983** (9.884)	0.000	-15.011* (8.707)	0.000	-19.245 (8.987)	0.000	-2.575 (2.436)	0.928	-2.166 (2.431)	0.115	2.170 (2.242)	8.760
IT equipment	0.059 (0.204)	1.061	0.084 (0.183)	1.088	0.145 (0.179)	1.156	0.218*** (0.061)	0.874	0.174*** (0.059)	1.190	0.103* (0.057)	1.109
Performance	-0.038 (0.192)	0.963	-0.094 (0.169)	0.910	0.023 (0.178)	1.023	-0.075 (0.050)	4.699	-0.053 (0.051)	0.948	-0.113** (0.050)	0.894
Bed size	0.440** (0.226)	1.552	0.215 (0.205)	1.240	0.380 (0.218)	1.463	-0.135* (0.076)	0.010	-0.081 (0.074)	0.922	-0.103 (0.075)	0.902
Academic	1.691 (1.531)	5.427	1.340 (0.419)	3.819	1.616 (1.420)	5.031	1.547*** (0.352)	1.060	1.546*** (0.354)	4.692	1.173*** (0.330)	3.231
Hospital	-7.698*** (1.298)	0.000	-7.196*** (1.167)	0.001	-8.303 (1.241)	0.000	-4.629*** (0.339)	0.380	-4.495*** (0.340)	0.011	-4.306 (0.318)	0.013
2006	1.728 (1.243)	5.632	2.198*** (0.852)	9.012	-0.364 (1.619)	0.695	0.058 (0.319)	0.443	0.457 (0.293)	1.579	0.498 (0.323)	1.645
2007	1.022 (1.221)	2.750	1.442* (0.794)	4.231	-0.774 (1.565)	0.461	-0.966** (0.320)	0.051	-0.633** (0.296)	0.531	-0.429 (0.319)	0.651
2008	-0.058 (1.301)	0.943	0.489 (0.895)	1.631	-1.753 (1.635)	0.173	-0.815** (0.341)	0.055	-0.543* (0.314)	0.581	-0.300 (0.341)	0.741
2009	-21.481 (5168)	0.000	-19.929 (3142)	0.000	-18.875 (894)	0.000	-2.970*** (0.375)	0.928	-2.684*** (0.341)	0.068	-2.174*** (0.368)	0.114
2010	-3.262** (1.292)	0.039	-2.691*** (0.881)	0.068	-4.871 (1.618)	0.008	-2.896*** (0.339)	0.874	-2.621*** (0.304)	0.073	-2.153*** (0.334)	0.116
LL ⁺	-361.98		-369.328		-373.846		-2283.34		-2275.82		-2319.64	

*Notes. Standard errors are in parentheses. p-values are represented by * Significant at $p < 0.1$, ** Significant at $p < 0.05$, *** Significant at $p < 0.01$*

**Hazard models are estimated using log likelihood(LL) functions and LL indicates the fit of the model with higher values indicating a better fit*

Table 7. Hazard model results by breach type (state level)

	Inside						Outside					
	Model (1)		Model (2)		Model(3)		Model (1)		Model (2)		Model(3)	
	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$	β_j	$h(t)$
Proactive Investment			-1.748 (1.141)	0.174					-0.988*** (0.222)	0.372		
Reactive Investment					0.346 (0.569)	1.413					-0.452** (0.184)	0.636
Security Investment	-0.762** (0.363)	0.467					-1.495*** (0.225)	0.224				
Proactive Law	-2.969** (1.427)	0.051					-2.511*** (0.449)	0.081				
Law	-0.368 (1.092)	0.692	-1.217 (1.098)	0.296	-0.722 (0.982)	0.486	-2.334*** (0.431)	0.097	-2.083*** (0.376)	0.125	-0.782*** (0.240)	0.458
Proactive x Law	0.596 (1.454)	1.815					1.571*** (0.496)	4.810				
SI x Law	0.667 (0.219)	1.950					0.044 (0.066)	1.045				
PI x Law			1.091 (1.138)	2.979					0.350** (0.156)	1.419		
RIx Law					0.146 (0.565)	1.157					-0.067* (0.033)	0.935
Controls												
Inverse Mills ratio	-8.770* (4.930)	0.000	-16.225*** (4.058)	0.000	-6.745* (3.849)	0.001	-3.016** (1.596)	0.049	-2.807* (1.384)	0.060	-1.384 (1.363)	0.250
IT equipment	0.019* (0.011)	1.020	0.024*** (0.006)	1.026	-0.003 (0.008)	0.997	0.045*** (0.007)	1.046	0.031*** (0.006)	1.031	0.021*** (0.005)	1.021
Performance	-0.001 (0.007)	0.999	-0.013*** (0.004)	0.989	-0.016*** (0.004)	0.984	0.038*** (0.007)	1.040	-0.003 (0.003)	0.997	-0.005** (0.002)	0.995
Bed size	0.001 (0.026)	1.001	0.024* (0.014)	1.019	-0.039** (0.016)	0.962	0.072** (0.020)	1.075	-0.002 (0.010)	0.998	-0.031*** (0.009)	0.969
Academic	0.198 (1.184)	1.219	0.512 (1.127)	1.669	-0.288 (1.134)	0.750	1.694 (0.199)	5.441	1.360*** (0.188)	3.898	1.439*** (0.181)	4.216
Hospital	-0.750*** (0.058)	0.463	-0.840*** (0.057)	0.431	-0.883*** (0.057)	0.414	-0.841*** (0.066)	0.431	-0.687*** (0.051)	0.503	-0.669*** (0.041)	0.512
2006	1.422* (0.768)	4.145	1.699** (0.770)	5.469	1.397* (0.782)	4.045	-0.087 (0.565)	0.916	-0.254 (0.555)	0.776	-0.277 (0.552)	0.758
2007	0.410 (0.761)	1.507	0.909 (0.764)	2.482	0.769 (0.775)	2.157	-0.866* (0.485)	0.421	-0.940* (0.476)	0.391	-0.861* (0.475)	0.423
2008	-0.772 (0.864)	0.462	-0.147 (0.870)	0.863	-0.150 (0.882)	0.861	-1.812*** (0.543)	0.163	-1.888*** (0.533)	0.151	-1.880*** (0.530)	0.153
2009	-17.163 (519)	0.000	-16.143 (556)	0.000	-15.644 (555)	0.000	-2.572*** (0.538)	0.076	-2.233*** (0.534)	0.107	-2.196*** (0.530)	0.111
2010	-2.038** (0.835)	0.130	-1.530* (0.841)	0.217	-1.292 (0.854)	0.275	-2.118*** (0.505)	0.120	-2.153*** (0.497)	0.116	-2.066*** (0.493)	0.127
LL ⁺	-600.442		-588.86		-595.635		-1754.54		-1768.81		-1793.00	

*Notes. Standard errors are in parentheses. p-values are represented by * Significant at $p < 0.1$, ** Significant at $p < 0.05$, *** Significant at < 0.01
Hazard models are estimated using log likelihood (LL) functions and LL indicates the fit of the model with higher values indicating a better fit.

Figure 1. Conceptual Framework

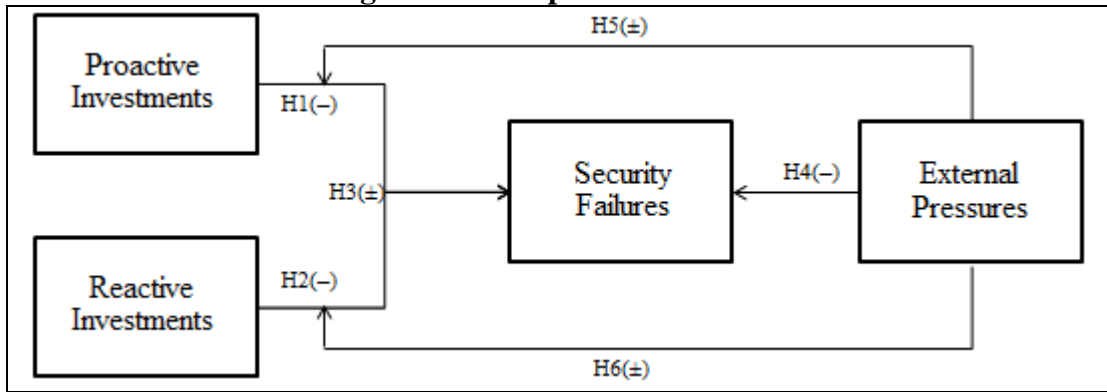


Figure 2. The probit models with information breaches

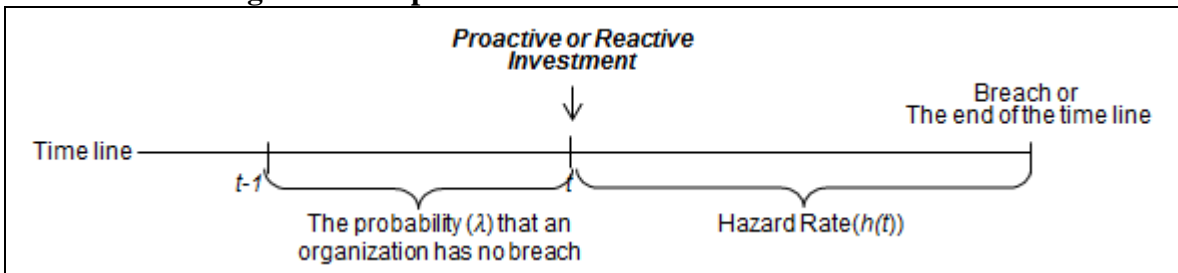


Figure 3. Hazard ratio at an organization and state levels

