An Organizational Learning Perspective on Proactive vs. Reactive Investment in Information Security*

Juhee Kwon and M. Eric Johnson
Tuck School of Business, Dartmouth College, NH
juhee.kwon@tuck.dartmouth.edu; m.eric.johnson@tuck.dartmouth.edu

Abstract

We present an empirical analysis of security investment in the healthcare sector to explore the impact of learning effects on breach performance. Employing organizational learning theory, we seek to identify how different types of security investment affect subsequent security failures. Our analysis is based on data from 2,386 healthcare organizations and benefits from data that have been gathered in a comparable manner across organizations and time. Using a Cox proportional hazard model for survival analysis, we find that proactive security investments are associated with longer intervals before subsequent breaches than reactive investments. Further, we find that external regulatory pressure can stimulate organizational learning and change. However, the interaction between external pressure and proactive investment reduces the positive effects of the investment. 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 be generalized to other industries.

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

---

* This research was partially supported by the National Science Foundation, Grant Award Number CNS-0910842, under the auspices of the Institute for Security, Technology, and Society (ISTS).

1. Introduction

In many areas of organizational performance, learning has been found to be an important element of 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 (Ittner, Nagar, & Rajan, 2001; Salomon & Martin, 2008). Others have examined how organizational experience interacts with external pressure, such as government regulation (Lynch, Buzas, & Berg, 1994; Plambeck & Wang, 2009). In particular, prior studies on product recalls have shown the importance of proactive strategies and the role of organizational volition on the learning effects from investments (Ittner, et al., 2001; Haunschild & Rhee, 2004). As the field of information security has evolved, researchers have also begun exploring the impact of organizational learning (Cavusoglu, Raghunathan, & Yue, 2008; Herath & Herath, 2008; Puhakainen & Siponen, 2010).

Security investments are often triggered by previous security failures or government regulation. Because breaches harm individuals through privacy violations and potential identity theft, both federal and state legislation mandate notification (Johnson 2009; Roberds et al. 2009; Romanosky et al. 2011). Such notifications are expensive and result in negative publicity (Kannan et al. 2007; Kolfal et al. 2010; Wang et al. 2008). These observations motivated us to employ organizational learning theory to investigate how proactive and reactive security investments differ for security improvement and how external pressures related to security failures affect organizational learning. Answering these questions will help policy makers and researchers better understand the potential impact of new regulation and the value of carrot (investment incentives) vs. stick (breach reporting) policies. We also consider the impact of information sharing among organizations and the economic incentive mechanisms for a public good like security (Gal-Or & Ghose, 2005).

We conduct our empirical analysis within the healthcare sector—examining the effects of security investments before and after security failures and the impact of those investments, along with external pressures, on subsequent security failures. Information security within the healthcare sector (Anderson, 1996) is an issue of growing importance. There have been many documented U.S. cases where patient information has been maliciously exploited by criminals seeking to commit medical and financial identity theft (Johnson, 2009; Lohmeyer, McCrory, & Pogreb, 2002). As vast patient information becomes accessible through electronic medical records (EMR), security becomes increasingly important. Federal regulations like HIPAA[2] and HITECH[3], as well as individual state regulations, have required providers to follow various guidelines concerning security failures. Thus, the healthcare industry provides a particularly appropriate context to investigate the impact of regulation on proactive (and voluntary) security investments. It also allows us to examine the public-goods nature of security.

In healthcare, 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 & 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

---

[2] *HIPAA : Health Insurance Portability and Accountability Act*
[3] *HITECH : Health Information Technology for Economic and Clinical Health Act*

organization level and for groups of organizations. Finally, our healthcare context benefits from data that have been gathered and accumulated in a comparable manner across organizations and time.

We begin in Section 2 by first examining the organizational learning literature that motivates our hypotheses. In Section 3, we present our research method and data collection. Section 4 provides our analysis followed by discussion and conclusions. Our 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, applying the 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.

2. Hypotheses Development

From the financial perspective, measuring ROI for security has proved particularly challenging because the success of such investment is "nothing happened" (Anderson, 2001; Behara, Derric, & Hu, 2006; Gordon & Loeb, 2002). On the other hand, the organizational learning perspective has viewed investment as the quest for improvement in the learning processes for problem-solving heuristics and techniques (Hauser & Clausing, 1988; Winter, 1994). Learning from investments enables people and their organizations to explore root causes of problems and to see potential opportunities for shaping a better future (Mukherjee, Lapre, & Van Wassenhove, 1998). Moreover, Attewell (1992) argued that the investment in advanced technologies should be considered a special category of innovative actions because of the burden of organizational learning they impose on employees. Hauschild and Rhee (2004) categorized investments into proactive and reactive approaches, with different organizational learning. The proactive approach argues that organizational learning occurs as a result of an organization's (proactive) innovative actions (Fine, 1986; Li & Rajagopalan, 1998). Reactive investments are triggered by failures that require remedial action (Marcellus & Dada, 1991).

Organizational learning also affects the link between IT 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. Implementing IT security controls in an organization arises from an investment decision that is proactively or reactively made. The know-how and technical knowledge associated with such IT security controls will be created by users via the process of learning by doing (Attewell, 1992). Therefore, the organizational learning would imply 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.*

In general, proactive investment is deployed by the waterfall approach in conventional software engineering (Frakes & Kang, 2005). The target domain (i.e., security) is analyzed, and then controls for the domain are defined and implemented considering foreseeable variations. This approach tends to require a large upfront investment—particularly with security because the threat models are constantly evolving, making it difficult to proactively prepare for every possible failure.

Therefore, rather than overinvest proactively, some organizations wait to observe attacks and use this knowledge to better allocate security spending (Bohme & Moore, 2010). A reactive strategy implies that an organization is responding to past experience so that the failures can be addressed efficiently and effectively. Bohmer and Moore (2010) suggest that increasing uncertainty results in reactive investment, because the uncertainty about the weakest link would cause firms using a proactive approach to overinvest. When uncertainty in the weakest links is very high, an organization does not know which asset to protect and so may choose to protect none until failures or weakest points are realized. Thus, in these cases, it may to be rational to under-invest 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 (Magnini, Ford, Markowski, & Honeycutt, 2007).

On the other hand, proactive approaches lie at the heart of an organization's strategy to gain competitive advantages. The launch of proactive investments requires a clear understanding of security vantage points (definition and vision), government and public expectations, perceived security concerns, and determinants of security. Gaining an understanding of these issues significantly contributes to improvement in organizational learning. As compared with industries like financial services, healthcare is generally less sophisticated and lags in adoption of the latest security technologies. This observation would lead one to conclude that the uncertainty over the weakest link in healthcare may be lower than in industries with a long history of cyber-attack (like financial service). Given similar uncertainties about the weakest links within the healthcare sector (and the learning required to understand the uncertainties), we hypothesize that the effect of proactive investments 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 government requirements on investment decisions. Understanding organizational responses to external pressures has implications for policy decisions within information security. Previous literature from various disciplines has investigated organizational responses to government-mandated changes (Majumdar & Marcus, 2001; Marcus, 1988; Saari, Bedard, Dufort, Hryniewiecki, & Theriault, 1993). Commonly, they have considered government requirements as the activation of attention that can make organizations focus on the 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 only 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, new state 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. 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, too much 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 & Rothschild, 1975; Winter, 1981) rather than assess security at all operational layers.

On the other hand, some 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 (cf. Rowe & Gallaher, 2006; Zollo & 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 & 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 affect learning from proactive and reactive investments and subsequently security performance (without hypothesizing a positive or negative affect). We hypothesize that:

HYPOTHESIS 5. *The external pressure influences the effect of proactive security investments on the reduction of subsequent security failure.*

HYPOTHESIS 6. *The external pressure influences the effect of reactive security investments on the reduction of subsequent security failure.*

3. Research Methods

We test our hypotheses using a hazard model.

The Hazard Model

Our data on security failures within healthcare organizations includes the breach date, allowing us to employ a statistical method that considers the dependence of the organization's security *survival* or *failure* on the explanatory variables. Hazard models are particularly useful for such analysis examining the impact of explanatory variables on the timing or probabilities of failure at the individual levels (Eliashberg, Singpurwalla, & Wilson, 1997; Kauffman, McAndrews, & Wang, 2000; Li, Shang, & Slaughter, 2010). For example, Eliashberg et al. (1997) developed a proportional hazard model to assess the size of a reserve needed by a manufacturer to meet future warrantee 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 proportional hazard model to relate software firms' capabilities to their failure rates. These studies have observed "time to events" and explored the effectiveness of a variety of explanatory variables. Among hazard models, the Cox proportional hazard model includes other attractive features. For example, the model: does not depend on distribution assumptions of survival time; provides flexibility for time dependent explanatory variables; and allows for hazard rate as an estimate of relative risk. Therefore, we use the Cox proportional hazard model to examine the duration between the effects of explanatory variables (i.e., security investment and regulatory requirement) and subsequent security failures.

Security Failure Analysis

The hazard function, $\lambda(t)$, 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 of investment until the either the event of interest – security failure – occurs or the end of the observation period. Thus, our hazard rates represent the relative risks of security failures within a time unit (where the time unit is one month). The hazard model is expressed as:

$$\lambda_i(t) = \lambda_0(t)e^{\sum_{j=1}^{K}\beta_j x_{ij}}$$

where β_j is a vector of unknown regression parameters to be estimated for j=1,…, K. The baseline hazard function $\lambda_0(t)$ involves time but not explanatory variables and the second component is the exponential functions with the sum of $\beta_j x_{ij}$, which involves explanatory variables but not time. 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, vice versa.

$$\frac{\lambda_i(t)}{\lambda_0(t)} = e^{\sum_{j=1}^{K} \beta_j x_{ij}}$$

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,$\lambda_i(t)$, of an individual (*i*) divided by the hazard, $c_i(t)$, of all the other organizations (R_i) (May, Hosmer, & Lemeshow, 2008).

$$L(\beta) = \prod_{i=1}^{N} \frac{e^{(\beta_1 x_{1i} + \cdots + \beta_k x_{ki})}}{\sum_{l \in R_i} e^{(\beta_1 x_{1l} + \cdots + \beta_k x_{kl})}} = \prod_{i=1}^{N} \frac{\lambda_i(t)}{c_i(t)}$$

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

$$LL(\beta) = \sum_{i=1}^{N} (\lambda_i(t) - c_i(t)) = \sum_{i=1}^{N} \beta_i (x_i - x_l) = \beta_0 + \beta_1 \widehat{x_{1\iota}} + \cdots + \beta_k \widehat{x_{k\iota}}$$

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

4. Empirical Analysis

Data Sources and Samples

We use data from the Healthcare Information and Management Systems Society (HIMSS) Analytics™ Database[4] from 2005 to 2009. During this period, HIMSS used a consistent database structure. The database provides information about the adoption of health information technology – 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,

[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.*

location, academic status, and so on. These data have been widely used in previous studies to examine the impact of healthcare information systems (Angst & Agarwal, 2009; Hillestad et al., 2005; Miller & Tucker, 2009). For the period of 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 indicate that all *p*-values are larger than 10% as seen in Table 1. Thus, we cannot reject the null hypothesis that two sample means are 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 Database [7].

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 implemented. HIMSS

[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.*
[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 also gathered staff and volunteers through sponsorship funding and donations.*

includes data on anti-virus, encryption, firewall, intrusion detection, user authentication, and spam filter.

We also 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 in 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 order to investigate the effect of regulatory requirements on security performance, we incorporated state security breach notification laws (*Law*) into our model. Data on state legislation 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 include lost-devices or accidently exposed healthcare information cases, as well as malicious insider activity. Second, *Outside* breaches 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 have been widely used to represent a healthcare organization's size and available resources. *Academic* and *hospital* are dummy variables to describe an organization type. If an organization includes an academic

[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.*

institute, *academic* is set to one; otherwise zero. *Hospital* has a value of 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 are 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.

5. Results

First, we assessed the correlations between the independent variables of the hazard model, and conducted a multicollinearity test using regression. 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 0.55 and 0.96, which are above the common cutoff threshold of 0.1 (Hair, Tatham, Anderson, & Black, 2005). The variance inflations (VIFs) of all variables are less than 1.82. 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.

Next, we ran the Cox Proportional hazard regression models to evaluate organization-specific variables and covariates as determinants of subsequent security failure. To evaluate covariates as determinants of interdependent security failures among organizations due to information sharing, the analyses were performed at both levels: an organization and state levels. While Model (1) tests the effect of overall security investments across all our analyses, Model (2) separately investigates the effects of proactive and reactive security investments.

Results from Hypotheses Tests

Table 4 and 5 report the estimates of the parameters (β_i) and hazard rates ($\lambda(t)$) for the models. Hypothesis 1 and 2 argued that proactive and reactive security investments reduce an investing organization's subsequent security failures. As shown in Table 4, the estimation yielded support for hypothesis 1 and 2 with negative coefficients for proactive and reactive security investments (-0.926 (*p<0.001*) and -0.363 (*p<0.05*), respectively). Note that the coefficient of proactive investment is much smaller than that of reactive. Their hazard rates have 0.396 in proactive and 0.696 in reactive. This simple observation implies that proactive security investments reduce security failures (reduce the likelihood of a security failure by about 60%) more than reactive ones (reduce the likelihood of a security failure by about 30%). We will more rigorously compare these in the following section. Additionally, as shown in Table 5, the state-level tests for Hypothesis 1 and 2 provide similar results with the coefficients of -5.476 ($p<0.001$, $\lambda(t)$=0.004) and -2.798 ($p<0.001$, $\lambda(t)$=0.061) for proactive and reactive investments, respectively. Proactive and reactive investments reduce subsequent security failures at both levels. Figure 1 plots the difference of the hazard rates (or failure rates) at the two different levels (i.e., organization and state). The graph shows that the hazard rates of both proactive and reactive investments are lower at a state level than at an organization level. The difference decreases at the state level of analysis. These results are consistent with both the theories of organizational learning and public goods.

We next compare the effect of proactive investments to that of reactive investments on subsequent security failures (Hypothesis 3). The above tests, which proactive and reactive investments were conducted as separate variables for Hypothesis 1 and 2, already demonstrated proactive investment has larger negative effect (coefficient) and smaller hazard rate than reactive investment. It is not uncommon for researchers to separately compare the effects of different types on a focal variable. 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) included an indicator, which represents a proactive type of security investments as one, to test the Hypothesis 3. The coefficient of a proactive type has -2.427($p<0.001$) at an organization level and -3.216 ($p<0.001$) at a state level. The coefficients of the proactive type are always negative at both an organization level and a state level. It indicates that proactive investments result in lower failure rates than reactive investments at both levels. Therefore, we can conclude that fewer security failures occur when an organization adopts proactive investments as opposed to reactive investments.

An external pressure, like government regulation, is another focal variable in the models. Hypothesis 4 argues that organizations learn from externally mandated requirements, which results in organizational improvement. We tests Hypothesis 4 by investigating the effects of breach notification laws on subsequent security failures. We find support for this hypothesis with Model (1) and Model (2). Model (1) shows the coefficients of the laws –1.848 ($p<0.001$, $\lambda(t)$=0.158) at an organization and -2.356 ($p<0.001$, $\lambda(t)$=0.095) at a state. Likewise, Model (2) has the negative coefficients -2.900 ($p<0.001$, $\lambda(t)$=0.055) and -1.276 ($p<0.001$, $\lambda(t)$=0.279). Thus, we conclude that externally mandated procedures are associated with improved security performance.

Finally, 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 an organization level, an external requirement attenuates the effects of proactive and reactive investments on subsequent security failures with positive coefficients 0.763 ($p<0.001$, $\lambda(t)$=2.145) and 0.433($p<0.05$, $\lambda(t)$=1.542). At a state level, the requirement does not significantly influence the effect of proactive investments with a positive coefficient 0.725, while it significantly increases the effect of reactive investments with a negative coefficient, -0.545 ($p<0.05$, $\lambda(t)$=0.58).

Extensions

Security breaches stem from both internal failures, such as accidental disclosure or malicious insiders, as well as external threats, such as malware and hacking. An issue we have not addressed is the learning associated with specific types of security failures. Organizations often focus on presenting external attacks rather than insider threats, even though insider threats can be equally harmful (Liu, Wang, & Camp, 2009). Our analysis thus far assumes that an organization's concern about security failure costs and willingness to learn are same for insider and outsider threats. However, prior literature supports the notion that an organization's perception and willingness to learn affects the actual learning and future performance (Ryu, Kim, Chaudhury, & Rao, 2005; Zakay, Ellis, & Shevalsky, 2004). Thus, if the organization views outside attacks as more important, they may focus more attention on them and indeed learn to better protect against them.

To investigate this question, we divided security failure into two groups: inside and outside. If larger concerns about a problem lead to greater effort to resolve the problem, we would expect the learning effect 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 support this prediction. The failure in preventing outside threats has significant negative associations with proactive and reactive security investments, but the failure in preventing inside threats have no significant association with the investments.

6. Implications and Conclusions

Organizational learning is believed to be driven by a combination of investments and external pressures (Ittner, et al., 2001; Li & 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. Our 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 is diminished. This implies that voluntary, proactive investments have the best performance. The findings have important implications both for 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 (that are more frequent) and thus may focus more investments on IT security to curb outsider threats rather than insider threats (Liu, et al., 2009; Liza, 2010). However, an organization might learn more from education or internal policies to prevent inside threats than from implementing technical controls.

In terms of social effects of organizational learning, our results show that learning by doing through proactive security investments relieves on economic incentives, whereas unilaterally mandated procedures do not have any economic incentive. Security investments induce learning by doing or learning through implementing controls, which typically involve many employees in learning. On the other hand, government requirements simply focus attention on the problem area rather than discovery and learning by doing. Therefore, while both proactive and reactive security investments have socially economic incentives in organizational learning, external pressure does not have significant social incentives.

Out results focus on the healthcare sector, where recent federal legislation mandates breach disclosure and data on security investments are available. However, we believe that our findings can be generalized to other industries, which face similar information risks.

While our paper has provided a number of interesting insights, some important issues remain for future research. First, we considered only the investments on IT security controls and did not address the issue of policies and training programs. While implementing controls such as training would have a direct learning effect, our study was more focused on indirect learning effects through learning by doing or learning by using IT security controls. Second, our model measured security investments as the number of IT security controls, and not the momentary amount of security investment. We also did not consider the cost of a breach, viewing all publically reported breaches as equally bad. Future research could also examine the potential interactions among the various security mechanisms to determine their joint effects on failure rates, and how the security investment changes as security management matures and knowledge increases. Furthermore, another possible study could examine whether all organizational failures affect learning, possibly by comparing breaches across different industries and different types of failure events (e.g., financial fraud). Finally, another limitation of our study is the limited time duration considered. This is a limitation of survival or hazard models in general. Using this approach, it is common to observe that some organizations never experience a failure within the study period. Longer study periods can help mitigate this limitation.

Despite these limitations, our results have implications for managers and researchers. Our results show 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 our 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.

References

Anderson, R.J. (1996). Security in Clinical Information Systems. *University of Cambridge*

Anderson, R.J. (2001). Why information security is hard - An economic perspective. *IEEE Computer Society, 17th Annual Computer Security Applications Conference Proceedings*, 358-365.

Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuation. *MIS Quarterly, 33*(2), 339-370.

Appari, A., & Johnson, M. E. (2009). Information Security and Privacy in Healthcare: Current State of Research. *International Journal of Internet and Enterprise Management.Enterprise Management*, Vol. 6, No. 4, 279-314.

Attewell, P. (1992). Technology Diffusion And Organizational Leraning - The Case of Business Computing. *Organization Science, 3*(1), 1-19.

Behara, R., Derric, C., & Hu, Q. (2006). *A Process Approach to Information Security:Lessons from Quality Management.* Paper presented at the Americas Conference on Information Systems (AMCIS).

Bohme, R., & Moore, T. (2010). The Iterated Weakest Link. *IEEE Security & Privacy, 8*(1), 53-55.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the Internet: Self-regulation or government regulation? *Business Ethics Quarterly, 16*(3), 323-342.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25*(2), 281-304. doi: 10.2753/mis0742-1222250211

Cox, D. R. (1972). Regression Models And Life-Tables. *Journal of the Royal Statistical Society Series B-Statistical Methodology, 34*(2), 187-&.

Eliashberg, J., Singpurwalla, N. D., & Wilson, S. P. (1997). Calculating the reserve for a time and usage indexed warranty. *Management Science, 43*(7), 966-975.

Fine, C. H. (1986). Quality Improvement And Learning In Productive Systems. *Management Science, 32*(10), 1301-1315.

Frakes, W. B., & Kang, K. (2005). Software reuse research: Status and future. *Ieee Transactions on Software Engineering, 31*(7), 529-536.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*(2), 186-208.

Gordon, L., & Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5*(4), 438.

Hair, J. F., Tatham, R. L., Anderson, R. E., & Black, W. (2005). *Multivariate Data Analysis* (6 edition ed.): Prentice Hall.

Haunschild, P. R., & Rhee, M. (2004). The role of volition in organizational learning: The case of automotive product recalls. *Management Science, 50*(11), 1545-1560.

Hauser, J. R., & Clausing, D. (1988). The House of Quality. *Harvard Business Review, 66*(3), 63-73.

Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems, 25*(3), 337-375. doi: 10.2753/mis0742-1222250310

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs, 24*(5), 1103-1117. doi: 10.1377/hlthaff.24.5.1103

Ittner, C. D., Nagar, V., & Rajan, M. V. (2001). An empirical examination of dynamic quality-based learning models. *Management Science, 47*(4), 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*, 71-89.

Kauffman, R. J., McAndrews, J., & Wang, Y. M. (2000). Opening the "black box" of network externalities in network adoption. *Information Systems Research, 11*(1), 61-82.

Li, G., & Rajagopalan, S. (1998). Process improvement, quality, and learning effects. *Management Science, 44*(11), 1517-1532.

Li, S. L., Shang, J., & 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), 631-654. doi: 10.1287/isre.1100.0281

Liu, D. B., Wang, X. F., & Camp, L. J. (2009). Mitigating Inadvertent Insider Threats with Incentives. In R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security* (Vol. 5628, pp. 1-16).

Liza. (2010). Managing Insider & Outsider Threats to IT Security & IT GRC. *Article Alley*. Retrieved from Article Alley website: http://www.articlealley.com/article_1702977_45.html

Lohmeyer, D. F., McCrory, J., & Pogreb, S. (2002). Managing information security. *The McKinsey Quarterly*. Retrieved from

Lynch, J. G., Buzas, T. E., & Berg, S. V. (1994). Regulatory Measurement And Evaluation of Telephone Service Quality. *Management Science*, *40*(2), 169-194.

Magnini, V. P., J. B. Ford, E. P. Markowski, E. D. Honeycutt Jr, (2007). The service recovery paradox: justifiable theory or smoldering myth? *Journal of Services Marketing*, Vol. 21 Iss: 3, pp.213 - 225

Majumdar, S. K., & Marcus, A. A. (2001). Rules versus discretion: The productivity consequences of flexible regulation. *Academy of Management Journal*, *44*(1), 170-179.

Marcellus, R. L., & Dada, M. (1991). Interactive Process Quality Improvement. *Management Science, 37*(11), 1365-1376.

March, J. G. (1991). Exploration and Exploitation in Organizational Learning. *Organization Science*, *2*(1), 71-87.

Marcus, A. A. (1988). Implementing Externally Induced Innovations - A Comparison of Rule-Bound And Autonomous Approaches. *Academy of Management Journal*, *31*(2), 235-256.

May, S., Hosmer, D. W., & Lemeshow, S. (2008). *Applied survival analysis: regression modeling of time-to-event data / David W. Hosmer, Stanley Lemeshow, Susanne May*. Hoboken, N.J: Wiley-Interscience.

Miller, A. R., & Tucker, C. (2009). Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records. *Management Science, 55*(7), 1077-1093. doi: 10.1287/mnsc.1090.1014

Mukherjee, A. S., Lapre, M. A., & Van Wassenhove, L. N. (1998). Knowledge driven quality improvement. *Management Science, 44*(11), S35-S49.

Ocasio, W. (1997). Towards an attention-based view of the firm. *Strategic Management Journal, 18*, 187-206.

Plambeck, E., & Wang, Q. (2009). Effects of E-Waste Regulation on New Product Introduction. *Management Science, 55*(3), 333-347. doi: 10.1287/mnsc.1080.0970

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Traning: An Action Research Study. *MIS Quarterly, 34*(4), 757-778.

Radner, R., & Rothschild, M. (1975). Allocation of Effort. [Article]. *Journal of Economic Theory, 10*(3), 358-376.

Rowe, B. R., & Gallaher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. *CiteSeerX*.

Ryu, C., Kim, Y. J., Chaudhury, A., & 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), 245-278.

Saari, J., Bedard, S., Dufort, V., Hryniewiecki, J., & Theriault, G. (1993). How Companies Respond To New Safety Regulations - A Canadian Investigation. *International Labour Review*, *132*(1), 65-74.

Salomon, R., & 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), 1266-1280. doi: 10.1287/mnsc.1080.0866

Shankar, V. (2006). Proactive and reactive product line strategies: Asymmetries between market leaders and followers. *Management Science*, *52*(2), 276-292. doi: 10.1287/mnsc.1050.0443

Winter, S. G. (1981). Attention Allocation and Input Proportions. *Journal of Economic Behavior & Organization*, *2*(1), 31-46.

Winter, S. G. (1994). *Organizing for continuous improvement: evolutionary theory meets the quality revolution*. New York: Oxford University Press.

Zakay, D., Ellis, S., & Shevalsky, M. (2004). Outcome value and early warning indications as determinants of willingness to learn from experience. *Experimental Psychology, 51*(2), 150-157. doi: 10.1027/1618-3169.51.2.150

Zollo, M., & Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. *Organization Science, 13*(3), 339-351.

Table 1. Two sample *t*-test

Measure	*t*-value	*p*-value
security investment	0.60	0.55
performance	-0.45	0.65
IT equipment	-1.42	0.16
bed size	-1.45	0.14

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.	0.08	0.27	0.00	1.00
Inside	1 if an inside (malicious and accidental) beach occurs; otherwise 0	0.02	0.15	0.00	1.00
Outside	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.	17.89	13.29	1.00	65.00
Security investment	The number of IT security controls implemented at different layers.	3.03	1.57	0.00	12.00
Proactive Investment	The number of security investments without a breach experience.	2.37	1.87	0.00	12.00
Reactive Investment	The number of security investments with a breach experience.	0.66	1.45	0.00	12.00
Proactive Type	1 if a security investment occurs without a breach experience, otherwise 0.	0.75	0.42	0.00	1.00
Law	1 if a state has breach notification laws, otherwise 0	0.85	0.35	0.00	1.00
Control variables					
IT equipment	Log (number of computers and laptops operated)	3.56	1.60	0.00	8.01
Performance	Log(Annual revenue)	19.74	1.91	14.52	24.01
Bed size	Log (number of beds)	5.03	1.00	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	0.26	0.00	1.00
years	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) Proactive Investment	1							0.64	1.54
(2) Reactive Investment	-0.57*	1						0.61	1.61
(3) Law	-0.13*	0.06*	1					0.96	1.03
(4) IT equipment	0.03*	0.12*	0.12*	1				0.55	1.81
(5) Performance	-0.3*	0.39*	0.05*	0.02	1			0.81	1.22
(6) Bed Size	-0.05*	0.13*	0.05*	0.67*	0.10*	1		0.54	1.82
(7) Academic	0.01*	0.05*	0.02	0.30*	-0.05*	0.31*	1	0.87	1.14
(8) Hospital	0.12*	0.05*	-0.01	-0.04	-0.00	-0.16	0.03*	0.83	1.20

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

Table 4. Hazard model results (organization level)

Explanatory variables	Organization Level (even=281) Model (1) β_j	Model (1) $\lambda(t)$	Model (2) β_j	Model (2) $\lambda(t)$	Hypotheses
Proactive Investment (PI)			-0.926*** 0.252	0.396	H1: Supported
Reactive Investment (RI)			-0.363** 0.179	0.696	H2: Supported
Security Investment (PI+RI)	-0.231** 0.120	0.793			
Proactive Type	-2.427*** 0.467	0.088			H3: Supported
Law	-1.848*** 0.282	0.158	-2.900*** 0.971	0.055	H4: Supported
Proactive Type x Law	2.219*** 0.494	9.205			
SI × Law	0.431** 0.129	1.540			
PI × Law			0.763*** 0.257	2.145	H5: Supported
RI× Law			0.433** 0.193	1.542	H6: Supported
IT equipment	0.016 0.063	1.017	0.158 0.104	1.172	
Performance	-0.167** 0.045	0.846	0.130 0.083	1.139	
Bed size	-0.018 0.084	0.982	-0.143 0.161	0.867	
Academic	0.542 0.302	1.720	-0.287 0.267	0.751	
Hospital	-4.244*** 0.266	0.014	-0.863*** 0.314	0.422	
2006	0.581* 0.306	1.789	-0.355 0.524	0.701	
2007	-0.396* 0.291	0.673	-0.628 0.497	0.534	
2008	-0.254* 0.304	0.775	-1.667*** 0.534	0.189	
2009	-1.713*** 0.428	0.180	-2.680*** 0.551	0.069	
2010	-1.616*** 0.333	0.199	-2.977*** 0.523	0.051	
Log likelihood (LL)*		-1210.5		-1212.7	

Notes. *Standard errors are in parentheses. p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.001*

**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)

Explanatory variables	State Level (even=281)				
	Model (1)		Model (2)		
	$\boldsymbol{\beta_j}$	$\lambda(t)$	$\boldsymbol{\beta_j}$	$\lambda(t)$	
Proactive Investment (PI)			-5.476*** 1.196	0.004	H1: Supported
Reactive Investment (RI)			-2.798*** 1.060	0.061	H2: Supported
Security Investment (PI+RI)	-4.482*** 0.891	0.011			
Proactive Type	-3.216*** 0.505	0.040			H3: Supported
Law	-2.356*** 0.504	0.095	-1.276** 0.712	0.279	H4: Supported
Proactive Type x Law	1.735*** 0.543	5.668			
SI × Law	-0.318* 0.201	0.727			
PI × Law			0.725 0.697	2.065	H5: Not Supported
RI× Law			-0.545** 0.242	0.58	H6: Supported
IT equipment	0.040 0.041	1.041	0.107** 0.051	1.112	
Performance	0.126*** 0.038	1.135	0.072 0.049	1.075	
Bed size	0.261*** 0.091	1.299	0.230*** 0.099	1.258	
Academic	0.113 0.253	1,120	-0.145 0.268	0.865	
Hospital	-2.875*** 0.317	0.056	-2.671*** 0.346	0.069	
2006	-0.364*** 0.511	0.695	-0.438 0.522	0.646	
2007	-1.360*** 0.467	0.256	-1.743*** 0.490	0.175	
2008	-2.386*** 0.500	0.092	-2.966*** 0.524	0.052	
2009	-3.295*** 0.507	0.037	-4.691*** 0.569	0.009	
2010	-1.916*** 0.472	0.147	-2.540*** 0.499	0.079	
Log likelihood (LL)*		-895.5		-900.5	

Notes. *Standard errors are in parentheses. p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.001*

**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 (event=86)				Outside (event=195)			
	Model (1)		Model (2)		Model (1)		Model (2)	
	$\boldsymbol{\beta_j}$	$\lambda(t)$	$\boldsymbol{\beta_j}$	$\lambda(t)$	$\boldsymbol{\beta_j}$	$\lambda(t)$	$\boldsymbol{\beta_j}$	$\lambda(t)$
Proactive Investment (PI)			-57.903 30.330	0.000			-0.792*** 0.258	0.453
Reactive Investment (RI)			-14.119 9.008	0.000			-0.280 0.182	0.755
Security Investment (PI+RI)	-0.477 0.591	0.621			-0.223* 0.119	0.800		
Proactive Type	-17.326 14.95	0.000			-2.313*** 0.486	0.099		
Law	-2.311 2.605	0.099	-47.459 27.030	0.000	-2.138*** 0.291	0.118	-2.322** 0.919	0.098
Proactive Type x Law	14.701 9.500	>1000			2.523*** 0.508	12.473		
SI × Law	0.827 0.601	2.287			0.404*** 0.131	1.499		
PI × Law			58.045 33.000	>1000			0.602** 0.263	1.826
RI× Law			14.544 8.710	>1000			0.200 0.203	1.221
IT equipment	-0.121 0.136	0.886	-0.094 0.137	0.91	0.002 0.069	1.003	0.141 0.112	1.152
Performance	-0.433*** 0.125	0.648	-0.391 0.119	0.677	-0.127** 0.050	0.880	0.201** 0.091	1.223
Bed size	0.188 0.189	1.207	0.183 0.191	1.2	0.022 0.091	1.023	-0.201 0.178	0.818
Academic	-1.370 1.138	0.254	-1.041 1.081	0.353	0.850*** 0.317	2.341	0.129 0.291	1.138
Hospital	-3.516*** 0.620	0.030	-4.195 0.639	0.015	-4.255*** 0.276	0.14	-0.991*** 0.350	0.371
2006	2.576** 1.126	13.145	2.444 1.117	11.519	0.159 0.326	1.173	-1.048* 0.631	0.351
2007	2.071** 1.068	7.931	1.983 1.065	7.267	-0.967 0.321	0.380	-0.873 0.549	0.418
2008	0.965 1.163	2.625	1.133 1.147	3.106	-0.413 0.318	0.661	-2.222*** 0.620	0.108
2009	-17.176 19.92	0.000	-20.356 13.977	0	-1.712*** 0.447	0.180	-2.786*** 0.607	0.062
2010	-0.830 1.216	0.436	-0.752 1.186	0.472	-1.639*** 0.353	0.194	-3.007*** 0.575	0.049
Log likelihood (LL)*		-186.1		-182.8		-997.1		-998.9

Notes. *Standard errors are in parentheses. p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.001*

**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 (event=86)				Outside (event=195)			
	Model (1)		Model (2)		Model (1)		Model (2)	
	$\boldsymbol{\beta_i}$	$\lambda(t)$	$\boldsymbol{\beta_i}$	$\lambda(t)$	$\boldsymbol{\beta_i}$	$\lambda(t)$	$\boldsymbol{\beta_i}$	$\lambda(t)$
Proactive Investment (PI)			-3.375* 1.989	0.034			-1.739*** 0.260	0.176
Reactive Investment (RI)			-1.950 3.258	0.142			-0.946*** 0.174	0.388
Security Investment (PI+RI)	-0.109 0.365	0.896			-0.672*** 0.152	0.510		
Proactive Type	-2.153** 1.134	0.116			-2.221*** 0.395	0.109		
Law	-0.626 0.858	0.534	-1.572 2.764	0.208	-2.553*** 0.218	0.078	-2.035*** 0.295	0.131
Proactive Type x Law	0.264 1.122	1.301			2.315*** 0.423	10.120		
SI × Law	0.665** 0.233	0.179			-0.119* 0.026	0.887		
PI × Law			-0.775 1.261	0.461			0.909*** 0.189	2.483
RI× Law			-0.322 2.844	0.725			-0.045*** 0.012	0.956
IT equipment	-0.025 0.016	0.975	0.353** 0.126	1.423	0.020*** 0.007	1.021	-0.022*** 0.008	0.979
Performance	-0.016 0.010	0.984	0.033 0.071	1.034	0.039*** 0.007	1.040	0.044 0.008	1.045
Bed size	-0.041 0.038	0.959	0.183 0.199	1.201	-0.028*** 0.010	0.972	-0.012*** 0.014	0.988
Academic	-0.084 1.057	0.919	-3.011** 1.262	0.049	0.823*** 0.309	2.279	0.945*** 0.307	2.574
Hospital	-6.155*** 0.680	0.002	-32.26** 11.66	0	-5.998*** 0.324	0.002	-6.545*** 0.292	0.001
2006	1.220* 0.569	3.388	0.878 3.712	2.406	-0.123 0.282	0.884	-0.258 0.279	0.773
2007	0.849 0.535	2.339	-1.364 3.738	0.256	-0.767** 0.264	0.464	-0.554** 0.261	0.575
2008	-0.516 0.656	0.597	-1.965 3.747	0.14	-0.804*** 0.322	0.447	-0.715** 0.313	0.489
2009	-15.500 53.373	0.000	-6.815* 4.013	0.001	-3.051*** 0.448	0.047	-2.989*** 0.443	0.05
2010	-2.767*** 0.787	0.063	-2.569 4.015	0.077	-1.678*** 0.317	0.187	-1.654*** 0.307	0.191
Log likelihood (LL)*		-101.4		-110.8		-752.0		-751.1

Notes. *Standard errors are in parentheses. p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.001*

**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. Difference between organization and state levels