SECURITY RESOURCES, CAPABILITIES AND CULTURAL VALUES: LINKS TO SECURITY PERFORMANCE AND COMPLIANCE[1]

Juhee Kwon and M. Eric Johnson
Center for Digital Strategies, Tuck School of Business, Dartmouth College
juhee.kwon@dartmouth.edu; m.eric.johnson@dartmouth.edu

Abstract

This study examines how security resources, capabilities, and cultural values influence security performance and perceived regulatory compliance. Using binomial and multinomial logit models, we analyze qualitative and quantitative survey data collected from 250 healthcare organizations. The results show that security resources and security capabilities are positively associated with compliance and security performance. Further, resources and capabilities complement each other, improving both compliance and performance. We also find that security audit capabilities are associated with increased breach disclosures, likely because such auditing helps organizations find, disclose and fix breach-related problems. In terms of cultural values, we find that top management support and expertise are significantly linked to compliance and security performance. Lastly, we find that collaborative cultures appear to foster compliance yet experience the same level of breaches. These results provide policy insight on effective security programs that harness resources, capabilities, and culture.

Keywords: *Security Resources, Security Capabilities, Compliance, Security Culture, Healthcare, Resource-based View*

[1] 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). We also acknowledge Kroll Fraud Solutions and the Health Information and Management Systems Society (HIMSS) Foundation for providing survey data.

SECURITY RESOURCES, CAPABILITIES AND CULTURAL VALUES: LINKS TO SECURITY PERFORMANCE AND COMPLIANCE

Introduction

Electronic health records (EHRs) have been identified as a key enabler of both healthcare quality improvement and cost reduction. The 2009 US HITECH Act created billions of dollars in incentives for healthcare providers to implement EHRs. However, as more records are moved into digital form, security of patient data has become a significant concern. As Fichman et al. (2011) note, patient data is highly personal, compounding the public fears of data breaches. Accordingly, as part of HITECH, Health and Human Services (HHS) implemented a new breach notification regime [2] that requires healthcare organization to publically post breach announcements, both in local news outlets and on HHS' website, for any data losses affecting 500 or more individuals. Additionally, HHS increased the severity of fines for HIPAA violations—both for inadvertent and willful disclosure of unsecured patient information. These new penalties, ranging up to $1.5M, are linked to the severity of the violation.

The new regulatory mandates and public concern have dramatically increased the pressure on healthcare providers to secure patient data. Besides fines and embarrassment, breached organizations also face significant reputational damage and remediation costs. However, even as organizations invest in security practices, questions remain concerning the effectiveness of different security practices and their impact on security performance (Cremonini and Nizovtsev 2009; D'Arcy et al. 2009). In the first two years of HHS breach reporting, over ten million patients' data have been exposed—in many cases by hospitals who had made significant security

[2] As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following website shows the breaches reported to the Secretary by breached healthcare organizations. See *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html*

investments. The limited success of security practices has been attributed to a range of issues including superficial implementation (Spears and Barki 2010), lack of complementarities between practices (Bharadwaj et al. 2007), and lack of emphasis on information security as a cultural value (Culnan and Williams 2009; Smith et al. 2010).

The adoption of security practices to offset potential information risks is a major challenge to many organizations because information risks originate at different layers in the IT infrastructure and within human resources. Thus, achieving information security requires adopting resources and developing capabilities at multiple layers; not only technology-based solutions—such as firewalls, anti-virus software, and intrusion detection systems—but also social alignment mechanisms—such as security policies, procedures, and education programs to convey users' roles and responsibilities (Kayworth and Whitten 2010). Recently, researchers and practitioners have further argued that security practices should be supported by an organizational culture that not only improves security awareness but also enhances the individuals' motivation to act responsibly and in accordance with firm policies (Johnson et al. 2009; Puhakainen and Siponen 2010; Spears and Barki 2010).

However, to our knowledge, there is little empirical evidence identifying the factors that differentiate between successful and unsuccessful implementation of security resources and the associated impact of security capabilities and cultural values (Cavusoglu et al. 2008). This paper aims to identify how security resources, capabilities, and cultural values influence security performance and perceived regulatory compliance. In doing so, we sharpen the theoretical characterization of "security performance" by unpacking the major sources of variation on security resources, capabilities, their complementarities, and cultural values.

Our results show that security resources and capabilities are positively associated with both compliance and security performance. Further, security resources and capabilities complement each other for better compliance and security performance. However, we find that security audit capabilities are associated with increased breach disclosures, while positively impacting perceived compliance. In terms of security cultural values, top management support and expertise significantly improve perceived compliance and security performance. Lastly, we find that collaborative cultures are associated with improved compliance yet have no impact on security performance. Our work contributes to the dearth of organizational-level security research. In addition, our analysis provides practical implication guidance for managers working to improve security and policy makers hoping to improve private-sector security.

Theoretical Development

Resource-based View

We employ the resource-based view perspective to develop a theoretical basis for security performance. The resource-based view links organizational performance to its resources and capabilities (Grant 1996; Wernerfelt 1984). It conceptualizes organizations as bundles of resources (Mahoney and Pandian 1992; Oliver 1997) that are likely to be heterogeneously distributed due to differences in organizational capabilities such as policies or procedures (Aral and Weill 2007). This heterogeneity drives differences in organization performance. The interaction of resources and capabilities imply that an organization adopts certain types of resources and, over time, develops resource-specific policies and procedures, which are defined as capabilities (Cohen and Levinthal 1990).

Maurer et al. (2011) extended the classical resource-based view to account for cultural values, creating a culturally informed perspective of the resource-based view. That view argues that very

similar strategies using the same resources and capabilities can result in diverse outcomes because of differences in an organization's cultural values. Therefore, it is difficult to know how resources and capabilities contribute to performance without understanding cultural differences tied to their internalization (Dierickx and Cool 1989; Maurer et al. 2011). These perspectives provide compelling theoretical reasons for investigating how security resources and capabilities are associated with an organization's goals for information security and the complementarities of security cultural values.

Security Resources and Capabilities

According to the resource-based view, large organizations are likely to have more resources than small ones (Marcus and Nichols 1999), such as IT security applications, procedures, and IT security staff (e.g., more highly skilled IT personnel than small organizations). These differences produce heterogeneous outcomes such as regulatory compliance and breach occurrences.

Although the resource-based view provides a helpful theoretical perspective on the heterogeneity of organizational performance, the definitions of resources and capabilities vary with each functional area of business. For example, in the manufacturing sector, resources could be manufacturing facilities, technology, or human resources. Capabilities could be systematic abilities in product development or operations (Rahmandad 2008). Capabilities are also defined as approaches to integrate equipment, technology, and other resources (Peng et al. 2008). In the IT area, researchers distinguish between technical components (e.g., IT security applications and devices) and nontechnical components (e.g., employee expertise, systematic processes, and procedures) (Aral and Weill 2007; Ross et al. 1996).

Following this categorization, we define information security resources as IT security applications and equipment, which become the framework for all security activities (cf.,

(Srivastava et al. 1998; Teece et al. 1997)). Historically, organizations have followed technically focused strategies for designing effective information security solutions because information security has been perceived to be a technical issue (Urbaczewski and Jessup 2002). IT security equipment and applications are generally believed to improve an organization's ability to monitor suspicious activities and prevent data breaches. Consequently, IT security resources likely increase security performance as well as perceived regulatory compliance. Thus, we hypothesize:

H1a: IT security resources are associated with regulatory compliance.

H1b: IT security resources are associated with security performance.

Because information security is not just technical but also a human issue, we study the strategic importance of information security by dividing security practices into security resources and capabilities. In our context, capabilities include security education programs, policies, and procedures, which are available and useful in detecting and responding to information threats. Capabilities can transform security resources into outputs of greater worth (Amit and Schoemaker 1993; Christensen and Overdorf 2000). In particular, information security requires a continuous process of identifying and preventing information security risks as well as auditing all information flow controls (i.e., countermeasures, safeguards).

Information security involves both preventing security breaches and auditing possible failure events (Weber 1999). Security researchers have argued that organizations improve information security through a combination of preventive and audit activities that reduce internal and external failures (Hong et al. 2003; Straub et al. 2008). These aspects have parallels in quality management where researchers have classified improvement initiatives into prevention (e.g., preventive maintenance, training, and process engineering) and appraisal activities (e.g.,

manufacturing inspection, audits, product testing) (Behara et al. 2006; Ittner and Larcker 1997; Ittner et al. 2001; Powell 1995). For example, Ittner et al. (2001) studied defect rates in manufacturing organizations and showed the impact of prevention/appraisal activities and compliance on quality performance. Such similarities between information security and quality management motivate us to utilize theory from quality management (Naveh and Erez 2004). Thus, we divide security capabilities into security and auditing practices and hypothesize:

H2a: Security capabilities are associated with regulatory compliance.

H2b: Security capabilities are associated with security performance.

H2c: Audit capabilities are associated with regulatory compliance.

H2d: Audit capabilities are associated with security performance.

Complementarities among Security Resources and Capabilities

The resource-based view further suggests that an organization's IT security, equipment, and technical measures such as organization-specific resources, can result in different performance due to organizational capabilities, which leverage the effects of resources. In the information security context, there is no one solution that can address and mitigate every known and unknown security threat across an entire organization. Best practice indicates that successful security programs employ a layered approach to resources and the policies/procedures related to those resources (Kayworth and Whitten 2010). For example, IT intrusion detection applications combined with security education programs likely create better outcomes than adoption of an application alone. The combination of security systems and abilities to use them enables the organization to communicate its ultimate goals and strategies, and leads to a common understanding of security strategies. In particular, IT security resources combined with embedded security capabilities form daily routines for enduring information security throughout

business operations. Organizations that successfully invest in such IT security resources and capabilities are thought to enjoy superior security performance (Bharadwaj et al. 2007; Tiwana and Konsynski 2010; Zhu 2004).

While resources and capabilities have their own roles, they are also interdependent and mutually support and reinforce each other (Tanriverdi 2006). The value of complementary resources and capabilities is greater than the sum of their individual values (Barua and Whinston 1998). Tanriverdi and Venkatraman (2005) argued that the relatedness and the complementarity of resources and capabilities could confer synergies. They explained that complementarities among the related resources and capabilities could create additional performance synergies (Tanriverdi and Venkatraman 2005). Likewise, IT security infrastructures, human resources, and third-party security management are complementary. Therefore, the complementarity of security resources and capabilities creates synergistic value (cf., (Ross et al. 1996)). The benefits of such an approach include improved compliance and fewer security incidents. This directly leads us to the following hypotheses:

H3a: The interaction between security resources and capabilities is associated with regulatory compliance.

H3b: The interaction between security resources and capabilities is associated with security performance.

Security Cultural Values

Kayworth and Whitten (2010) suggested that the underlying values about information security mesh with the values of the organization. Since an organization's members are likely to behave in ways consistent with cultural values, the values should be developed to align with organizational strategies. Organizations that recognize the dynamic interplay between their

resources, capabilities, and cultural values in the face of organizational issues can enhance their performance (Maurer et al. 2011). In particular, information security as an enterprise-wide issue requires cultural change and action on the part of all employees. Since all employees must realize the value of information security as an empowering function for goal achievement, a security-aware culture should be seeded. Security cultural values influence security practices delivered across an organization as well as guide employees to comply with the practices.

There is increasing interest in creating security cultures, which instill security practices into an organization, as a sub-unit of organizational culture (Lacey 2010; Malcolmson 2009). Security cultures raise awareness and motivate individuals to act responsibly and in accordance with policy (Culnan and Williams 2009; Smith et al. 2010). Although many regulatory regimes provide detailed checklists, such compliance will not likely produce security without a strong security culture that reflects the maturity and operational posture of security. Since a security culture is important to raise security awareness and motivate individuals to act responsibly, organizations implementing the same security practices may still have very different security performance based on their security culture. We examine organizational cultural values reflected by top management support (Barr and Glynn 2004; Hoffman and Hegarty 1993), top management expertise (Alavi et al. 2005), and collaboration (Rai et al. 2009).

Top Management Support. Organizations mirror the values and attitudes of their key executives as they set strategic direction (Porter 1980), develop policies (Selznick 1957), and manage those policies through day-to-day implementation (Cyert and March 1963). An organization's approach to value-laden issues is a projection of its executives' perspectives (Goodpaster and Matthews 1982). In practice, the nature of a security culture is largely determined by the leadership of top management (McFadzean et al. 2007). The political climate will influence the

tone for any security practice, which frequently faces employees' resistance to restrict or monitor their activities. Organizations have used various means to motivate employees' acceptance and internalization of security practices. To achieve this, top management needs to fully support and ensure that all facets of the organization—including reward and penalty systems, organizational structure, training, communication, and processes—reflect its values and beliefs. Thus, top management is a key component and a vital force for successful implementation and execution of information security practices.

H4a: The level of top management support is associated with regulatory compliance.

H4b: The level of top management support is associated with security performance.

Top Management Expertise. Expertise (i.e., experience, skills, and knowledge) is another important characteristic of organizational learning (Palomeras and Melero 2010; Song et al. 2003). Focusing on functional expertise of top managers offers a generalizable way of identifying which top managers influence innovations. Moreover, top management expertise serves as a limit on the areas in which top management is willing to understand existing or potential risks and allocate resources. Credibility, based on top management expertise, affects the believability or organizational commitment to their strategies (in this case, claims that an issue is significant for the organization) (Dutton and Ashford 1993). Top management groups differ in terms of the breadth and depth of expertise in various issue domains, and the differences affect their issue processing (Thong et al. 1996). When top management has expertise regarding some up-to-date technology or in-depth insights about potential risks, the expertise could enhance their initiatives for resolving the risks. Thus, the success of information security efforts is dependent, in part, on whether the risks are related to top management's expertise. When such relatedness occurs, an organization's attention is more easily secured because top managers can better

understand an issue and may feel more competent to take effective action (Hoffman and Hegarty 1993). In particular, information security requires in-depth understanding of laws and regulations to oversee security activities across an organization as well as security technologies. The following hypotheses are based on the importance of top management expertise on technologies, policies, and regulations in information security:

H5a: The level of top management expertise is associated with regulatory compliance.

H5b: The level of top management expertise is associated with security performance.

Collaboration. Since all employees, not only those in the security department, should be involved in utilizing the security systems and procedures, a collaborative security culture is important in achieving compliance and preventing security incidents (Paul et al. 2004). Collaborative security cultures require structures that empower an organization's departments to share information and to make important decisions together or take actions regarding the weakest links in their own daily operations. In the healthcare sector, patient information is shared as patients move between different departments of the hospital (e.g., emergency, surgery, radiology) and it is also shared between back-office groups like laboratories, billing, and collection. (Appari and Johnson 2010). Compliance and security requires the utilization of information to be understood among all departments. Thus, collaborative security cultures result in better compliance and security performance, implying the following hypotheses.

H6a: The level of collaboration between departments, which share data across an organization, is associated with regulatory compliance.

H6b: The level of collaboration between departments, which share data across an organization, is associated with security performance.

Compliance and Security Performance

The goals of a security program include regulatory compliance as well as secure operations (i.e., preventing breaches) (Bulgurcu et al. 2010; Johnston and Hale 2009; Kayworth and Whitten 2010; von Solms 2005;). Security regulations require organizations to evaluate security risks and to manage those risks. However, organizations focused on simply satisfying minimal compliance standards may be less secure than the others who exceed compliance (or even organizations who invest appropriately to mitigate organization-specific risks, but fail to achieve compliance on every security element).

Prior research identifies two key explanations for the relationship between compliance and performance. First, drawing from fear appeal theories (Johnston and Warkentin 2010), some degree of fear arousal induces a motivation for compliance to alleviate possible threats, which would be both punishments for noncompliance and potential loss arising from actual security incidents. Johnston and Warkentin (2010) argued that fear appeals do impact individuals' behavioral intentions to comply with security mandates. Further, since noncompliance results in fines, public disclosure, stock price volatility, and loss of business, security regulations motivate organizations. Thus, although many organizations consider compliance a burden, compliance can work as a catalyst for improving actual security performance.

Second, at the organizational level, regulatory compliance means that the organization is responsive to evaluate and manage information security risks. It is expected that such organizational responsiveness will be positively related to security performance (cf., (Joshi 2010)). For instance, if an organization complies with internal policies and legal requirements, security improves via the adoption of practical solutions that respond to regulatory requirements.

Such practical solutions might allow organizations to sustain consistent practices and effectively defend against illegal practices (Liberti 2008). This leads to the following hypothesis.

H7: Higher regulatory compliance results in higher security performance.

Data Collection and Measures

Data Sample and Variables

We draw data from the Kroll/HIMMS[3] hospital survey on patient data safety (Kroll/HIMSS 2010). This telephone-based survey of 250 healthcare organizations, polled respondents on hospital security practices, perceived compliance, and security performance. Respondents included IT executives, Chief Security Officers (CSO), Health Information Management (HIM) Directors, Compliance Officers and Privacy Officers. Table 1 provides descriptive statistics for the variables in our analysis.

Response Variables. To test the hypotheses, we employed two types of response variables: *Compliance* and *Security Performance.* For *Compliance*, we used a scale of one to seven on perceived compliance with five security regulations: HITECH, HIPAA, State Security Laws, Red flags, and CMS Regulations. We used it as a response variable as well as a mediator. *Security Performance* is measured by whether an organization experienced any breach occurrence in the past twelve months.

Independent Variables. Our independent variables include *security resources, capabilities,* and *cultural values* (i.e., top management support, expertise, and collaboration). The number of adopted IT security applications and devices represents *security resources*. *Security capabilities*

[3] Kroll is a leader in healthcare data security and has helped some of the largest healthcare providers in the country respond to data security breaches. The survey was conducted in partnership with HIMSS (Healthcare Information and Management Systems Society), the leading organization representing the health information management systems and services industry.

measures the existence of security policies/procedures, educational courses, hiring practices, and audit practices. We divided *security capabilities* into security and audit capabilities. The number of adopted security policies, education, and hiring practices estimates *security capabilities*, while the number of adopted monitoring activities represents *security audit capabilities*. Appendix A shows the detailed assignment of security resource and capabilities.

Cultural values include top management support for information security, top management expertise, and the level of collaboration among departments. Top management support and collaboration are measured on a scale from one to seven. As a binary variable, top management expertise is 1 if a top executive in charge of information security has the title Chief Security Officer (CSO), Chief Privacy Officer (CPO), or Chief Compliance Officer (CCO), otherwise 0.

Control Variables. We also included control variables commonly used in health economics to control for the size and type of organization including *bed size* and *healthcare organization type* (including *critical access, general medical,* and *academic). Bed size* is measured by the number of licensed beds. *Critical access, general medical,* and *academic* are all (exclusive) dummy variables that describe the organization type. *General med* is 1 if an organization is a general medical institute, *critical access* is 1 if it is a critical access institute, *academic* is 1 if it includes an academic program; otherwise zero.

Research Methodology

Our model examines the effects of security resources and capabilities on compliance and security performance along with the mediating effect of compliance (Baron and Kenny 1986). Further, it identifies the complementary effects between security practices on compliance and security performance. The conceptual framework, as shown in Figure 1, includes two stages. One stage

examines the effects of security resources, capabilities, and compliance with a multinomial logit model on security performance. The other identifies the role of compliance as a mediator using a binomial logit model (cf., (Ba and Pavlou 2002)).

As two response variables, security performance and compliance are discrete and the residuals are not normally distributed. The logit approach allows the prediction of discrete variables by a mix of continuous and discrete predictors. Further, the logit model does not require any distributional assumptions on the predictors (the predictors do not have to be normally distributed, linearly related or have equal variance in each group) (Hosmer and Lemeshow 1992).

First, the binomial logit model describes the relationship between multiple independent variables (i.e., security practices, capabilities, and compliance) and security performance. Security performance is expressed as the probability of breach occurrence, using a binary variable ("*no data breach*" or "*one or more than one breach*").

$$security_i = \begin{cases} 0, & no\ data\ breach \\ 1, & otherwise\ (more\ than\ one\ breach) \end{cases}$$

Our model predicts the probability of "*no data breach*", denoted $p_i = P\ (security_i = 0|\theta)$, given the parameters($\theta$). The probability of no data breach is predicted by fitting the data to a logistic function, given by

$$P(security_i = 0|\theta) = \frac{e^{security_i(\theta)}}{1 + e^{security_i(\theta)}}$$

The odds in favor of the event is the quantity, (p_i / (1- p_i)). The logarithm of the odds is the logit of the probability, $P(security_i = 0|\theta)$. Thus, using the logistic function:

$$\text{logit}(p_i) = \log\left(\frac{\frac{e^{security_i(\theta)}}{1+e^{security_i(\theta)}}}{1-\frac{e^{security_i(\theta)}}{1+e^{security_i(\theta)}}}\right) = security_i(\theta), \quad where$$

$$security_i(\theta) = \beta_0 + \beta_1 ITSec_i + \beta_2 SecPol_i + \beta_3 Audit_i + \gamma_1 TopMgmt_i + \gamma_2 Expertise_i + \gamma_3 Collaboration_i + \delta Compliance_i + \sum_k \eta_k Controls_k + \varepsilon_i \quad (1)$$

Equation (1) investigates only the main effects of the explanatory variables on security performance. We further examine the complementary effect between security resources and capabilities. The effect of IT security practices on security performance may differ based on the adoption of security policies/procedures. Accordingly, the probability of no breach can be extended with the functions of the main effects and the interaction terms. However, when interaction terms are included in the model, multicollinearity is likely. Thus, we performed our analysis of two-way interactions on the hypothesized variables using an alternative model. Equation (2) involves forming multiplicative terms as moderator variables to examine the effects of the complementarities between security practices and security performance as

$$security_i(\theta) = \beta_0 + \beta_1 ITSec_i + \beta_2 SecPol_i + \beta_3 Audit_i + \beta_4 (ITSec_i * SecPol_i) + \gamma_1 TopMgmt_i + \gamma_2 Expertise_i + \gamma_3 Collaboration_i + \delta Compliance_i + \sum_k \eta_k Controls_k + \varepsilon_i \quad (2)$$

We model security performance as measured by breach occurrence (a binary variable). An organization's compliance can also be modeled as a discrete integer (i.e., one-to-seven scale) that indicates a level of compliance. The logit model can be extended beyond the analysis of a binomial variable to the analysis of categorical variables with more than two categories (Menard 2001). Mathematically, the extension of the binomial logit model to the multinomial model is straightforward.

$$compliance_i = \begin{cases} 1, a\ level\ of\ compliance = 1 \\ 2, a\ level\ of\ complaince = 2 \\ \dots \\ 7, a\ level\ of\ complaicne = 7 \end{cases} \quad (M=1 \dots 7)$$

Note that when M=2, it becomes the logit model for the binomial response. For compliance with a number of categories (M), the multinomial logit model requires the calculation of M-1 equations,

$$P(compliance_i = h|\theta) = \frac{e^{compliance_i(\theta)}}{1 + \sum_{h=1}^{M-1} e^{compliance_i(\theta)}}, \ h = 1,2, \dots, M-1$$

Like the binomial logit model for security performance, the multinomial logit regression models of probability, $P(compliance_i = h|\theta)$ are represented by

$$compliance_i(\theta) = \beta_0 + \beta_1 ITSec_i + \beta_2 SecPol_i + \beta_3 Audit_i + \gamma_1 TopMgmt_i + \gamma_2 Expertise_i + \gamma_3 Collaboration_i + \sum_k \eta_k Controls_k + \varepsilon_i \quad (3)$$

$$compliance_i(\theta) = \beta_0 + \beta_1 ITSec_i + \beta_2 SecPol_i + \beta_3 Audit_i + \beta_4 (ITSec_i * SecPol_i) + \gamma_1 TopMgmt_i + \gamma_2 Expertise_i + \gamma_3 Collaboration_i + \sum_k \eta_k Controls_k + \varepsilon_i \quad (4)$$

Equation (3) investigates the effects of security resources, capabilities, and cultural values on compliance. Equation (4) further examines whether security resource and capabilities complement each other for better compliance.

Results

First, we assessed the correlations between the explanatory variables of the logit models. Table 2 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 0.22 and 0.96, which are above the common cutoff threshold of

0.1 (Hair et al. 2005). The variance inflations (VIFs) of all variables are less than 4.64. A usual threshold of VIFs is 10.0, which corresponds to a tolerance of 0.1. Therefore, we concluded that multicollinearity is not a concern for our models.

Figure 2 depicts the results of the model. Table 3 and 4 provide the coefficient estimates and odds for the models. H1a and H1b argue that the adoption of security resources is related to compliance and security performance. As shown in Table 3 and 4, the adoption of security resources significantly improved both compliance and security performance (β_1 = 1.497 and 1.162 at p<0.01) with odds ratios, 4.47 and 3.20, respectively, supporting H1a and H1b.

We separately examined the effects of two types of security capabilities: security and audit capabilities. For security prevention the estimates yielded by both models support H2a and H2b with positive coefficients (β_2= 0.889 and 1.161 at $p<0.01$) for compliance. On the other hand, while the effect of security audit capabilities positively affected compliance (β_3 = 1.112 at $p<0.01$) supporting H2c, it was significantly and negatively related to the probability of no data breach (β_3 = -2.675 at $p<0.01$) with an odds ratio of 0.07. This odds ratio (less than one) indicates that the odds of a breach increased when security audit capabilities increased. Generally, security audit capabilities are related to monitoring or detecting intrusions or illegal activities. Therefore, if an organization develops security audit capabilities, it may better find and report intrusions than others that do not realize they have been breached due to a lack of monitoring and detecting practices.

Further, we investigated the complementary effect between security resources and capabilities. In Tables 3 and 4, Models (2) and (4) respectively include the interaction terms of security resources and prevention capabilities. The analysis supports both H3a and H3b with β_4 = 0.624 at $p<0.01$ and 0.424 at $p<0.05$. These results imply that the interaction of security

resources and prevention capabilities increased regulatory compliance and security performance more than either type alone. In other words, the effect of security resources become greater when implemented in conjunction with proper education, hiring practice, policies and procedures.

We next investigated the effects of security cultural values including top management support, expertise, and collaboration. As we expected, top management support consistently had positive coefficients (γ_1= 0.188 at p <0.01 and 0.160 at p < 0.05) for compliance and security performance supporting H4a and H4b. Likewise, top management expertise increased the level of compliance and security performance with γ_2= 0.562 at p<0.01 and 0.251 at p< 0.1, respectively. Note that top management support and expertise have higher positive coefficients for regulatory compliance and lower *p*-values than those for security performance. It can be inferred that when top management provided more support and had higher security expertise, an organization's belief that it complied with the regulations increased more than its actual security performance.

On the other hand, collaboration among the departments did not have any significant effect on security performance, whereas it significantly increased compliance (γ_3= 0.613 at p<0.01) supporting H6a. Thus, a highly collaborative culture is associated with increased data breach risks due to more information sharing among organizational members, while possibly contributing to effective remediation or ex-post response activities. This result is also consistent with the previous argument that a top-down approach to information security has a higher probability of success for several reasons including dedicated funding, a clear planning and implementation process supported by upper-management, and the means for influencing organizational culture (Culnan et al. 2008; Whitman and Mattord 2011).

We further investigated whether security performance differs with the level of compliance. The results (δ, 0.269 and 0.233 at $p<0.01$) support H7. However, the coefficients of regulatory compliance are less than one fourth those of security resources and capabilities. This implies that an organization's security performance depended on its security practices more than its belief about regulatory compliance. Therefore, we suggest that an organization should focus on strategies to adopt proper practices and their complementarities by analyzing and mitigating weak security links rather than simply satisfying regulatory requirements.

The Number of Data Breaches

The above analysis of security performance simply considered the occurrence of a breach in the last 12 months, but not the breach severity. To include the severity (as measured by the number of data breaches in the past 12 months) we employed a multinomial logit model with the number of data breaches as the dependent variable.

$$breach_i = \begin{cases} 0, no\ data\ breach \\ 1, one\ breach\ occured \\ \dots \\ 10, ten\ breaches\ occurred \end{cases} \qquad (N=1 \dots 10)$$

The results were consistent with those of the binomial logit model except in the case of compliance. As Table 5 shows, security resources, security capabilities, and their complementarity are associated with decreased breach occurrences, while security audit capabilities is positively associated with data breaches. In terms of security cultural values, higher top management support and expertise resulted in fewer breaches. The impact of collaboration was not significant (although it has positive coefficients). However, compliance did not have a significant effect the severity of data breaches (while it significantly increased the probability of no data breach in the binomial logit model).

Reverse Causality

Our results suggest that security practices are associated with both compliance and security performance. However, questions remain about the mechanisms and direction of causality in the study. Perhaps instead of security practices causing better security performance or compliance, "secure organizations" adopt more security practices. In an econometric model, a loop of causality between the independent and dependent variables leads to endogeneity. We tested for reverse causality in our data. Hausman's test was used to check for the presence of measurement error with the available instrumental variables, which included an organization's strategic planning for potential breaches such as training, debrief processes after breaches, security consultation, and others. If a more secure organization tries to be more prepared and planned, the number of the planned practices is less correlated to breach occurrence and more related to the adopted practices. The Hausman test revealed that ordinary least squares (OLS) was preferred over both two-stage least squares (2SLS) and three-stage least squares (3SLS) with *p*-value, 0.56 and 0.73, respectively. Thus, it appears that reverse causality is not driving the results: adopting more security resources and prevention capabilities leads to better performance. Nonetheless, our efforts to disentangle causality have been limited by the lack of instrumental variables for security practice adoption at the organization-level. There may be some causality in both directions—certain organizational security characteristics make security practice adoption more likely.

Discussions and Conclusions

This study examined how security resources and capabilities influence regulatory compliance and security performance. We utilized qualitative and quantitative survey data provided by senior IT managers from 250 healthcare organizations. The data provides a snapshot of patient

information security in the surveyed organizations. We categorized security practices into security resources and capabilities, and further incorporated security cultural values to identify how compliance and security performance can be influenced by security cultural differences.

We found that IT security resources and capabilities positively affected security performance and regulatory compliance. Further, the complementarity of security resources and capabilities improved compliance and security performance more than that of either type of control alone. Security audit capabilities were positively associated with regulatory compliance, but also positively associated with reported breach incidents. For regulatory compliance, security audits had the strongest effect among security resources and capabilities. Compliance with data protection regulations required organizations to do more to find, disclose and fix breach-related problems. These tasks correspond with security audit capabilities including detection, notification and ex-post response cost activities. Thus, adopting more audit capabilities likely leads to higher compliance, while also resulting in the detection of more data breaches.

Compliance, as a mediator, was positively associated with the probability of no data breach in the binomial logit model, although its effect was the smallest among the explanatory variables. Moreover, an organization's compliance was not related to the number of data breaches that an organization experienced. This indicates that the severity of data breaches does not vary with an organization's belief about regulatory compliance (although the belief is associated with the likelihood of any data breach occurrence). Thus, we suggest that mitigating the severity of data breaches depends more on security resources and capabilities rather than regulatory compliance.

Our results imply that policy makers should focus on providing guidelines to invest in developing a combination of security resources, capabilities, and cultural values, rather than simply impose single-solution compliance requirements regardless of organizational

heterogeneity. In particular, we found that the complementary effects of security practices significantly enhanced compliance and security performance. Thus, we conclude that organizations that balance investment between security resources and capabilities can achieve a higher level of compliance and security performance.

Although our research provides a new perspective on security performance variation, it has some limitations. First, our measures were based on ordinal self-reported data from security managers in healthcare organizations. These measures might be vulnerable to respondents' subjective assessments of their organizations and to single respondent bias. Second, actual security performance was measured by the number of data breaches. The financial loss or breach remediation cost could provide additional insight on the effects of various security practices

Acknowledgement: The authors are grateful to the ICIS 2011 reviewers and participants for many valuable comments that helped improve the empirical analysis and presentation of the material.

References

Alavi, M., Kayworth, T. R. , and Leidner, D. E. 2005. "An empirical examination of the influence of organizational culture on knowledge management practices," *Journal of Management Information Systems* (22: 3), pp. 191-224.

Amit, R., and Schoemaker P. 1993. "Strategic Assets and Organizational Rent," *Strategic Management Journal* (14: 1), pp. 33-46.

Appari, A., and Johnson, M. E. 2010. "Information security and privacy in healthcare: current state of research," *International Journal of Internet and Enterprise Management* (6: 4), pp. 279 - 314.

Aral, S., and Weill, P. 2007. "IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation," *Organization Science* (18: 5), pp. 763-780.

Ba, S. L., and Pavlou, P. A. 2002. "Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior," *MIS Quarterly* (26: 3), pp. 243-268.

Baron, R. M., and Kenny, D. A. 1986. "The Moderator Mediator Variable Distinction in Social Psychological-Research - Conceptual, Strategic, and Statistical Considerations," *Journal of Personality and Social Psychology* (51: 6), (1986), pp. 1173-1182.

Barr, P. S., and Glynn, M. A.2004. "Cultural variations in strategic issue interpretation: Relating cultural uncertainty avoidance to controllability in discriminating threat and opportunity," *Strategic Management Journal* (25: 1), pp. 59-67.

Barua, A., and Whinston, A. B. 1998. "Decision support for managing organizational design dynamics," *Decision Support Systems* (22: 1), pp. 45-58.

Behara, R., Derric, C., and Hu,Q. 2006. "A Process Approach to Information Security:Lessons from Quality Management," in *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Acapulco, México.

Bharadwaj, S., Bharadwaj, A., and Bendoly, E. 2007. "The performance effects of complementarities between information systems, marketing, manufacturing, and supply chain processes," *Information Systems Research* (18: 4), pp. 437-453.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rational-based Beliefs and Information Security Awareness," *MIS Quarterly* (34: 3), pp. 523-548.

Cavusoglu, H., Cavusoglu, H., and Son, J. 2008. "What Drive Organizations to Invest in Information Security Controls? How Do Investments Improve Information Security Performance?" in *Proceedings of Workshop on Information Systems and Economics (WISE)*, Paris, France.

Christensen, C. M., and Overdorf, M. 2000. "Meeting the challenge of disruptive change," *Harvard Business Review* (78: 2), pp. 66-79.

Cohen, W. M., and Levinthal, D. A. 1990. "Absorptive-Capacity- A New Perspective on Learning and Innovation," *Administrative Science Quarterly* (35: 1), (1990), 128-152.

Cremonini, M., and Nizovtsev, D. 2009. "Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers," *Journal of Management Information Systems* (26: 3), (2009), pp. 241-274.

Culnan, M.J., Foxman, E.R., and Ray, A.W. 2008. "Why IT Executives should Help Employees Secure their Home Computers," *MIS Quarterly Executive* (7:1), pp. 49-56.

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly* (33: 4), pp. 673-687.
Cyert, R. M., and March, J. G. 1963. *A Behavioral Theory of the Firm*, Englewood Cliffs, NJ: Prentice-Hall.
D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach Prentice *Information Systems Research* (20:1), pp. 79-98.
Dierickx, I., and Cool, K. 1989. "Asset Stock Accumulation and Sustainability of Competitive Advantage," *Management Science* (35: 12), pp. 1504-1511.
Dutton, J. E., and Ashford, S. J. 1993. "Selling Issues to Top Management," *Academy of Management Review* (18: 3), pp. 397-428.
Fichman, R., Kohli R., and Krishnan, R. 2011. "The Role of Information Systems in Healthcare: Current Research and Future Trends," *Information Systems Research,* (22: 3), pp. 419-428.
Goodpaster, K. E., and Matthews, J. B 1982. "Can a Corporation have a Conscience," *Harvard Business Review* (60: 1), pp. 132-141.
Grant, R. M. 1996. "Toward a knowledge-based theory of the firm," *Strategic Management Journal* (17: 4), pp. 109-122.
Hair,J.F., Tatham, R.L., Anderson, R.E., and Black, W. 2005. *Multivariate Data Analysis*, Prentice Hall.
Hoffman, R. C., and Hegarty, W. H. 1993. "Top Management Influence on Innovations – Effects of Executive Characteristics and Social Culture," *Journal of Management* (19: 3), pp. 549-574.
Hong, K.S., Chi, Y.P., Chag, L.R., and Tang, J.H. 2003. "An Integrated System Theory of Information Security Management," *Information Management & Computer Security* (11: 5), pp. 243-250.
Hosmer, D. W., and Lemeshow, S. 1992. *Applied Logistic Regression*, WILEY Inter-Science.
Ittner, C. D., and Larcker, D. F. 1997. "The performance effects of process management techniques," *Management Science* (43: 4), pp. 522-534.
Ittner, C. D., Nagar, V., and Rajan, M. V. 2010. "An empirical examination of dynamic quality-based learning models," *Management Science* (47: 4), pp. 563-578.
Johnson, M. E., Goetz, E., and Pfleeger, S. L. 2009. "Security through Information Risk Management," *IEEE Security & Privacy* (7: 3), pp. 45-52.
Johnston, A. C., and Hale, R. 2009. "Improved Security through Information Security Governance," *Communications of the ACM* (52: 1), pp. 126-129.
Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34: 3), pp. 549-566.
Joshi, A. W. 2010. "Salesperson Influence on Product Development: Insights from a Study of Small Manufacturing Organizations," *Journal of Marketing* (74: 1), pp. 94-107.
Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive* (9: 3), pp. 163-175.
Kroll/HIMSS 2010, "HIMSS Analytics Report: Security of Patient Data." Kroll Fraud Solutions, Nashville, TN, May.
Lacey, D. 2010. "Understanding and transforming organizational security culture," *Information Management & Computer Security* (18: 1), pp. 4-15.

Liberti, L. 2008. *Survey Results: Reduce the Cost of Compliance While Strengthening Security*, Security Management Newsletter, (availabe at http://www.ca.com/files/articles/ secure0808_ survey_on_compliance.pdf).

Mahoney, J. T., and Pandian, J. R. 1992. "The Resource-based View within the Conversation of Strategic Management," *Strategic Management Journal* (13: 5), pp. 363-380.

Malcolmson, J. 2009. *What is security culture? does it differ in content from general organisational culture?* 2009 IEEE 43rd International Carnahan Conference on Security Technology(ICCST), Zurich, Switzerland.

Marcus, A. A., and Nichols, M. L. 1992. "On the edge: Heeding the warnings of unusual events," *Organization Science* (10: 4), pp. 482-499.

Maurer, C., Bansal, P., and Crossan, M. 2011. "Creating Economic Value Through Social Values: Introducing a Culturally Informed Resource-Based View," *Organization Science* (22: 2), pp. 432-448.

McFadzean, E., Ezingeard, 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: 5), pp. 622-660.

Menard, S. 2001. *Applied Logistic Regression Analysis*. Thousand Oaks, CA, Sage, 2001.

Naveh, E., and Erez, M. 2004. "Innovation and attention to detail in the quality improvement paradigm," *Management Science* (50: 11), pp. 1576-1586.

Oliver, C. Sustainable competitive advantage: Combining institutional and resource-based views. *Strategic Management Journal* (18: 9), pp. 697-713.

Palomeras, N. and Melero, E. 2010. "Markets for Inventors: Learning-by-Hiring as a Driver of Mobility," *Management Science* (56: 5), pp. 881-895.

Paul, D. L., and McDaniel, R. R. 2004. "A field study of the effect of interpersonal trust on virtual collaborative relationship performance," *MIS Quarterly* (28: 2), pp. 183-227.

Peng, D. X., Schroeder, R. G., and Shah, R. 2008. "Linking routines to operations capabilities: A new perspective," *Journal of Operations Management* (26: 6), pp. 730-748.

Porter, M. E. *Competitive strategy*. New York: Free Press.

Powell, T. C. 1995. "Total Quality Management as Competitive Advantage - A Review and Empirical Study," *Strategic Management Journal* (16: 1), pp. 15-37.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34: 4), pp. 757-778.

Rahmandad, H. 2008. "Effect of delays on complexity of organizational learning," *Management Science* (54: 7), pp. 1297-1312.

Rai, A., Maruping, L. M., and Venkatesh, V. 2009. "Offshore Information Systems Project Success: The Role of Social Embeddedness and Cultural Characteristics," *MIS Quarterly* (33: 3), pp. 617-641.

Ross, J. W., Beath, C. M., and Goodhue, D. L. 1996. "Develop long-term competitiveness through IT assets," *Sloan Management Review* (38: 1), pp. 31-43.

Selznick, P. 1957. "Law and the Structures of Social-Action," *Administrative Science Quarterly* (2: 2), pp. 258-261.

Smith, S., Winchester, D., Bunker, D., and Jamieson, R. 2010. "Circuits of Power: A Study of Mandated Compliance to An Information Systems Security De Jure Standard in A Government Organization," *MIS Quarterly* (34: 3), pp. 463-486.

Song, J., Almeida, P., and Wu, G. 2003. "Learning-by-hiring: When is mobility more likely to facilitate inter-firm knowledge transfer?" *Management Science* (49: 4), pp. 351-365.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34: 3), pp. 503-522.
Srivastava, R. K.,Shervani, T. A., and Fahey, L. 1998. "Market-based Assets and Shareholder value: A Framework for Analysis," *Journal of Marketing* (62:1), pp. 2-18.
Straub,D. W., Goodman, S. E., and Baskerville, R. 2008. *Information security: policy, processes, and practices*. M.E. Sharpe.
Tanriverdi, H. 2006. "Performance Effects of Information Technology Synergies in Multibusiness Firms," *MIS Quarterly* (30: 1), pp. 57-77.
Tanriverdi, H., and Venkatraman, N. 2005. "Knowledge Relatedness and the Performance of Multibusiness Firms," *Strategic Management Journal* (26: 2), pp. 97-119.
Teece, D. J., Pisano, G., and Shuen, A. 1997. "Dynamic Capabilities and Strategic Management," *Strategic Management Journal* (18: 7), pp. 509-533.
Thong, J. Y. L., Yap, C. S., and Raman, K. S. 1996. "Top Management Support, External Expertise and Information Systems Implementation in Small Businesses," *Information Systems Research* (7: 2), pp. 248-267.
Tiwana, A., and Konsynski, B. 2010. "Complementarities between Organizational IT Architecture and Governance Structure," *Information Systems Research* (21: 2), pp. 288-304.
Urbaczewski, A., and Jessup, L. M. 2001. "Does Electronic Monitoring of Employee Internet Usage Work?" *Communications of the ACM* (45:1), pp. 80-83.
von Solms, S. H. 2005. "Information Security Governance - Compliance Management vs Operational Management," *Computers & Security* (24: 6), pp. 443-447.
Weber, R. 1999. *Information System Control and Audit*, Prentice-Hall, 1999.
Wernerfelt, B. 1984. "A Resource-based View of the Firm," *Strategic Management Journal* (5: 2), pp. 171-180.
Whitman, M. E., and Mattord, H. J. 2011. *Principles of Information Security, Course Technology*.
Zhu, K. 2004. "The Complementarity of Information Technology Infrastructure and e-Commerce Capability: A Resource-based Assessment of their Business Value," *Journal of Management Information Systems* (21:1), pp. 167-202.

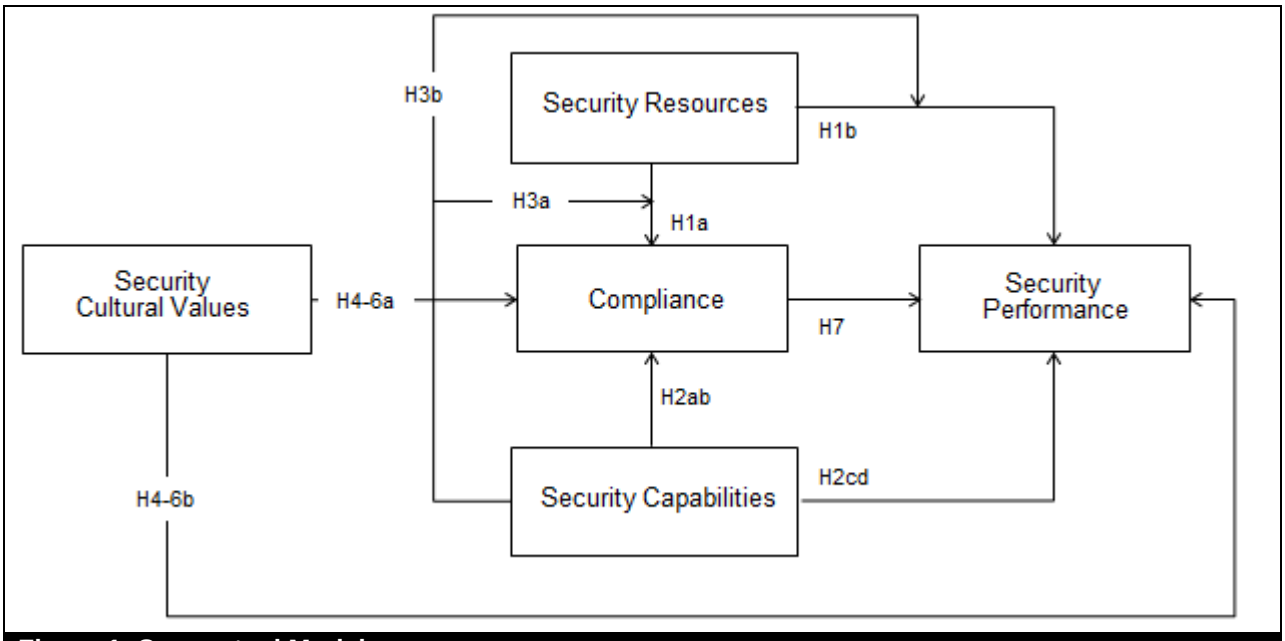

Figure 1. Conceptual Model

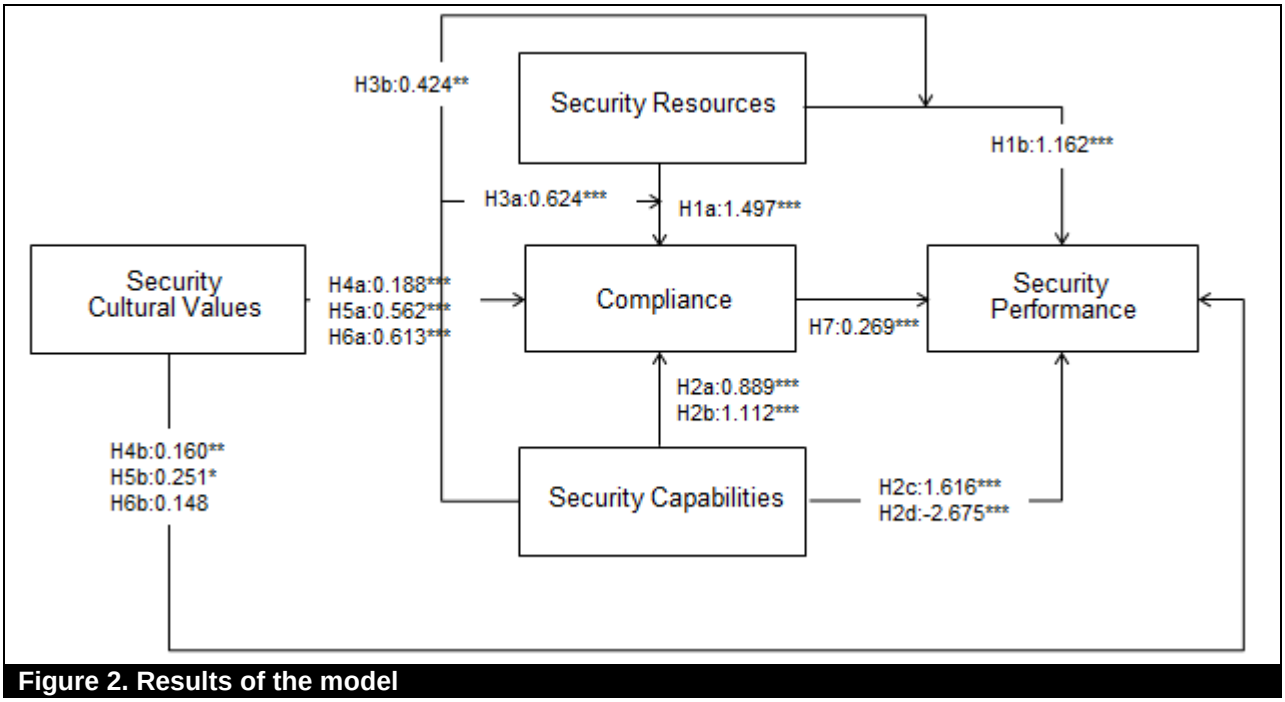

Figure 2. Results of the model

Notes. *p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at p <0.01*

Table 1. Descriptive statistics for key variables					
Variable	**Description (n=250)**	**Mean**	**StdD**	**Min**	**Max**
breach	The number of data breaches experienced	0.64	1.91	0	10
security	1 if an organization experienced any breach, otherwise 0.	0.18	0.39	0	1
compliance	An organization's compliance for HITECH/ARRA, HIPPA, state security laws, CMS, and Red flags rule	6.31	1.04	1	7
IT Security systems	The adopted IT security controls such as IT security applications, physical measures, and data access, to safeguard patient information = (IT security applications+physical measures+data access)/3	0.94	0.13	0.33	1
Security prevention	The adopted security practices such as HR, Education, and data assurance , to safeguard patient information = (HR+Education+ data assurance policies/procedures)/3	0.71	0.30	0	1
Security audit	The adopted procedures and processes to monitor patient information flow. = (System Audit+Audit policies+Audit log+Regular Audit+Regular review)/5	0.81	0.25	0	1
Top Mgmt. Support	The support level of a top executive in charge of information security.	6.39	1.11	0	7
Top Mgmt.Expertise	1, if a top executive in charge of information security is Chief Security Officer (CSO), Chief Privacy Officer (CPO), or Chief Compliance Officer (CCO), otherwise 0.	0.50	0.50	0	1
Collaboration	The level of collaboration between the departments, which manage clinical, financial and demographic information	5.96	0.96	2	7
Control variables					
Critical Access	1 if a type of an organization is Critical Access, otherwise 0.	0.33	0.50	0	1
General Med	1 if a type of an organization is General Med, otherwise 0.	0.56	0.47	0	1
Academic	1 if a type of an organization is Academic, otherwise 0.	0.04	0.50	0	1
Bed Size	1, If the bed size of an organization is under 100. 2, If the bed size of an organization is between 100 and 299. 3, If the bed size of an organization is above 300.	1.63	0.20	1	3

Notes. *p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at p <0.01.*

Table 2. Correlation matrix for independent variables

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	TOL	VIF
1) breach	1.00												
2) compliance	-0.09	1.00										0.86	1.16
3) IT Security	0.04	0.14	1.00									0.81	1.23
4) Prevention	**-0.14**	**0.21**	**0.25**	1.00								0.79	1.26
5) Audit	**0.08**	**0.20**	**0.33**	**0.37**	1.00							0.73	1.38
6) Top Mgmt. Support	**-0.07**	**0.16**	**0.19**	**0.13**	**0.12**	1.00						0.84	1.19
7) Top Mgmt. Expertise	**-0.09**	**0.09**	0.00	0.00	**-0.08**	0.02	1.00					0.96	1.05
8) Collaboration	**-0.07**	**0.30**	**0.11**	**0.27**	**0.27**	**0.35**	-0.01	1.00				0.76	1.32
9) Critical Access	**-0.11**	**-0.11**	**-0.22**	**-0.11**	**-0.23**	**-0.12**	**0.10**	**-0.10**	1.00			0.24	4.13
10) General Med	**0.08**	**0.07**	**0.24**	**0.11**	**0.24**	**0.15**	-0.05	**0.10**	**-0.79**	1.00		0.22	4.64
11) Academic	**0.06**	0.05	0.00	-0.02	**0.09**	0.00	0.04	0.03	**-0.14**	**-0.23**	1.00	0.53	1.87
12) Bed Size	**0.09**	0.04	**0.24**	0.01	**0.23**	**0.12**	-0.02	0.04	**-0.62**	**0.53**	**0.31**	0.49	2.04

Note. *Values in bold represent statistically significant p value at 0.05*

Table 3. The Multinomial logit model for regulatory compliance

Variable	Model (1)			Model (2)			Hypotheses
$P(compliance_i = h \mid \theta)$	β	Std Err	Odd Ratio	β	Std Err	Odd Ratio	
Security Resources							
IT Security Systems	1.497***	0.509	4.470	0.944*	0.529	2.569	H1a: Supported
Security Capabilities							
Security Prevention	0.889***	0.210	2.433	0.754***	0.214	2.125	H2a: Supported
Security Audit	1.112***	0.262	3.041	0.909***	0.267	2.481	H2b: Supported
Complementarities							
IT Security × Security Prevention				0.624***	0.157	1.865	H3a: Supported
Security Culture							
Top mgmt support	0.188***	0.055	1.207	0.148***	0.056	1.160	H4a: Supported
Top mgmt expertise	0.562***	0.125	1.753	0.545***	0.126	1.725	H5a: Supported
Collaboration	0.613***	0.070	1.847	0.608***	0.070	1.837	H6a: Supported
Control Variables							
Type							
Critical Access	-0.403***	0.161	0.668	-0.377**	0.162	0.686	
General Med	-0.282**	0.131	0.754	-0.276**	0.132	0.759	
Academic	0.182	0.285	1.199	0.186	0.289	1.204	
Size	0.044	0.125	1.044	0.082	0.126	1.086	
Intercept (Com=1)	-7.576***	0.658	0.001	-7.017***	0.672	0.001	
Intercept (Com=2)	-5.879***	0.641	0.003	-5.301***	0.656	0.005	
Intercept (Com=3)	-4.393***	0.635	0.012	-3.807***	0.652	0.022	
Intercept (Com=4)	-3.397***	0.646	0.033	-2.800***	0.663	0.061	
Intercept (Com=5)	-2.841***	0.662	0.058	-2.238***	0.679	0.107	
Intercept (Com=6)	-2.134***	0.704	0.118	-1.528**	0.720	0.217	
Pseudo R-square			*0.312*			*0.321*	
-2LL			*2,286.930*			*2,279.824*	

Notes. *p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at p <0.01*

Table 4. The Binomial logit model for security performance (the probability of no breach)

Variable	Model (3)			Model (4)			Hypotheses
$P(security_i=0\|\theta)$	β	Std Err	Odd Ratio	β	Std Err	Odd Ratio	
Security Resources							
IT Security Systems	1.162***	0.337	3.197	1.011***	0.340	2.749	H1b: Supported
Security Capabilities							
Security Prevention	1.616***	0.262	5.034	1.561***	0.261	4.763	H2c: Supported
Security Audit	-2.675***	0.458	0.069	-2.648***	0.453	0.071	H2d: Supported
Complementarities							
IT Security × Security Prevention				0.424**	0.177	1.528	H3b: Supported
Security Culture							
Top mgmt support	0.160**	0.070	1.167	0.173**	0.071	1.189	H4b: Supported
Top mgmt expertise	0.251*	0.164	1.372	0.264*	0.165	1.303	H5b: Supported
Collaboration	0.148	0.093	1.126	0.110	0.094	1.116	H6b: Not Supported
Compliance	0.269***	0.081	1.308	0.233***	0.082	1.263	H7 : Supported
Control Variables							
Type							
Critical Access	0.467**	0.213	1.596	0.482**	0.212	1.619	
General Med	-0.139	0.155	0.870	-0.165	0.156	0.848	
Academic	-0.698**	0.303	0.497	-0.689**	0.300	0.502	
Size	-0.009	0.151	0.991	0.006	0.150	1.006	
Intercept	-2.387***	0.791	0.092	-2.081***	0.803	0.125	
Pseudo R-square			*0.151*			*0.166*	
-2LL			*1,010.594*			*998.698*	

Notes. *p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at p <0.01*

Table 5. The Multinomial logit model for the number of data breaches

Variable	Model (5)			Model (6)			Hypotheses
$P(breach_i=h\|\theta)$	β	Std Err	Odd Ratio	β	Std Err	Odd Ratio	
Security Resources							
IT Security Systems	1.708***	0.352	5.519	1.276***	0.360	3.581	H1b: Supported
Security Capabilities							
Security Prevention	1.859***	0.280	6.419	1.660***	0.247	5.261	H2c: Supported
Security Audit	-2.652***	0.433	0.071	-2.977***	0.464	0.051	H2d: Supported
Complementarities							
IT Security x Security Prevention				0.565***	0.175	1.759	H3b: Supported
Security Culture							
Top mgmt support	0.169**	0.071	1.184	0.173**	0.071	1.189	H4b: Supported
Top mgmt expertise	0.393**	0.165	1.481	0.264*	0.165	1.303	H5b: Supported
Collaboration	0.052	0.093	1.054	0.110	0.094	1.116	H6b: Not Supported
Compliance	0.097	0.081	1.101	0.108	0.082	1.114	H7 : Not Supported
Control Variables							
Type							
Critical Access	0.261	0.217	1.299	0.332	0.217	1.394	
General Med	-0.307*	0.160	0.736	-0.255*	0.157	0.775	
Academic	-0.698**	0.291	0.497	-0.678**	0.289	0.508	
Size	-0.335**	0.151	0.715	-0.311**	0.152	0.733	
Intercept (breach=0)	-0.737	0.801	0.478	-0.626	0.813	0.535	
Intercept (breach=1)	0.028	0.801	1.029	0.152	0.813	1.164	
Intercept (breach=2)	0.827	0.805	2.286	0.966	0.816	2.628	
Intercept (breach=3)	1.087	0.807	2.964	1.229	0.818	3.419	
Intercept (breach=5)	1.340*	0.810	3.818	1.486*	0.821	4.421	
Intercept (breach=6)	1.493*	0.812	4.451	1.643**	0.824	5.170	
Pseudo R-square			*0.162*			*0.170*	
-2LL			*1,532.551*			*1,524.168*	

Notes. *p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at p <0.01*

Appendix

A. The descriptive statistics of security practices adopted.				
Variable		**Label**	**Mean**	**Std Dev**
Security Resources	IT Security	IT security applications	0.95	0.22
		Physical security measures	0.94	0.23
		Data access controls	0.94	0.23
Capabilities	Security	Ensuring that patient is who they say they are	0.91	0.28
		Formal security education courses	0.83	0.37
		Hiring practices-third party (i.e. background checks)	0.51	0.50
	Audit	Regular audits are conducted of systems that generate/collect/transmit patient data	0.86	0.34
		Specific policy in place to monitor electronic patient health information access and sharing	0.87	0.34
		IT audit logs are created and analyzed for inappropriate access to patient data	0.83	0.38
		Regular audits are conducted for processes where patient info is shared with external organizations	0.74	0.44
		Regular scheduled meetings are conducted to review status of data security policies	0.77	0.42