

# THE IMPACT OF SECURITY PRACTICES ON REGULATORY COMPLIANCE AND SECURITY PERFORMANCE<sup>1</sup>

*Research-in-Progress*

**Juhee Kwon**

Center for Digital Strategies

Tuck School of Business

Dartmouth College

Hanover, NH 03755

juhee.kwon@tuck.dartmouth.edu

**M. Eric Johnson**

Center for Digital Strategies

Tuck School of Business

Dartmouth College

Hanover, NH 03755

m.eric.johnson@tuck.dartmouth.edu

## **Abstract**

*This study examines how a healthcare organization's security practices (including IT controls, policies, education, and hiring practices) influence their perceived 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. Healthcare organizations must focus on preventing breaches (which results in brand damage and direct remediation costs) as well as complying with government regulation (to avoid indirect costs, including fines and penalties). Using hierarchical linear modeling (HLM), we examine how specific security practices improve regulatory compliance, protect patient information, and minimize the impact of a breach incident. The results show that audit policies are positively associated with perceived regulatory compliance and security policies are associated with security performance. We also find that the interaction of both audit and security policies has a more significant effect than either type alone. Surprisingly, an organization's level of compliance is not significantly associated with actual security performance. This study contributes to demonstrating which security practices can help the organizations comply with the regulations and the effects of security practices and regulatory compliance on information security performance. This can provide healthcare organizations with strategic guidelines to improve their regulatory compliance and security performance.*

**Keywords:** Security, Compliance, Healthcare, HITECH, HIPPA

---

<sup>1</sup> 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 sharing survey data.

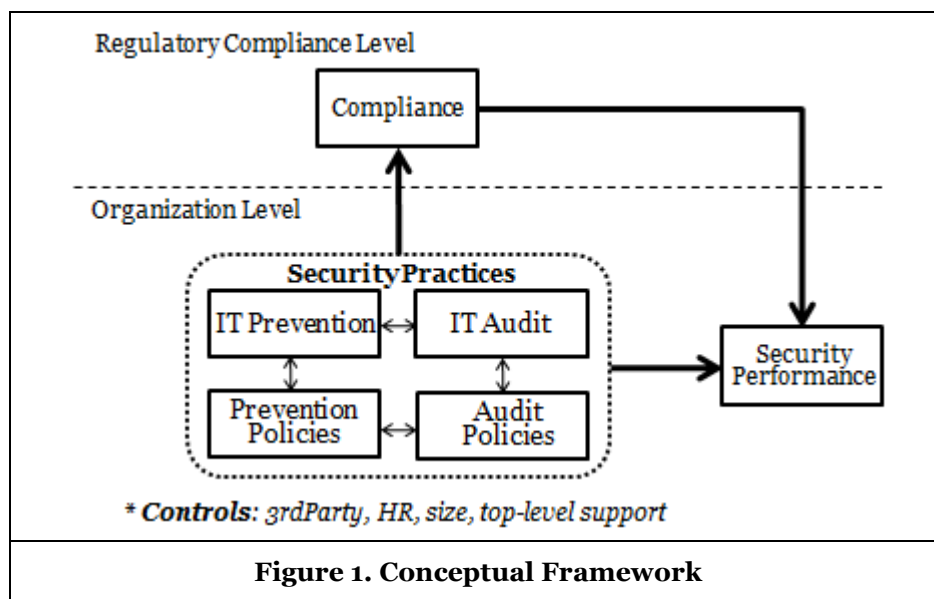
## Introduction

A growing level of awareness of healthcare information security in the U.S. has led to increased regulation and changes in security practices to comply with the new rules. However, a survey<sup>2</sup> by the US Department of Health and Human Services (HHS) noted that many respondents were still confused by the varying applications and interpretations of both federal (HITECH/HIPPA) regulations and state security laws. The regulations allow hospitals significant latitude in developing their security practices. This variation must be addressed to achieve national goals of widespread interoperable electronic health information exchange.

Researchers and practitioners have argued that organizations must be strategic in their approach to information security and regulatory compliance because security practices and budgets need to reflect various dimensions of evolving security threats (Johnston and Warkentin 2010; Kayworth and Whitten 2010; Spears and Barki 2010). However, organizations have focused on the primary role of technology in designing effective security solutions. Many have worried that organizations overemphasize simple checklists of technical parts rather than striving to deploy various solutions in protecting patient information (Puhakainen and Siponen 2010). However, it is not clear what such a strategy looks like in practice or how organizations actually achieve both proper regulatory compliance and security management.

This study examines how specific security practices improve regulatory compliance, protect patient information, and minimize the impact of a breach incident. Further, we investigate whether the level of compliance actually affects security performance. We formalize hypotheses describing the relationship between security practices, performance, and regulatory compliance.

Our results suggest that security prevention and audit polices are positively associated with security performance and perceived regulatory compliance, respectively. We also find that the interaction of both prevention and audit policies has a more significant effect than either type alone. This study contributes to demonstrating which security practices can help the organizations comply with the regulations and how security practices and regulatory compliance affect information security performance. This can provide healthcare managers build strategic guidelines to improve their regulatory compliance and security performance.



**Figure 1. Conceptual Framework**

<sup>2</sup> In June 2005, the US Department of Health and Human Services (HHS) published the *Summary of Nationwide Health Information Network Request for Information Responses*, which contained responses from 512 organizations and individuals.

Purpose	Type	Variables	Security Practices
Prevention	Security Prevention IT Controls	<i>IT Prevention</i>	IT Applications
			Technical IT Security Measures
			Data Access Minimization
	3 <sup>rd</sup> Party IT Controls	<i>ITthird</i>	Utilization of Tools to Secure Patient Information
	Security Prevention Policies	<i>Prevention</i>	Security Policy
			Ensuring that Patient Is Who They Say They Are
	HR Policies	<i>iHR</i>	HR Monitors Completion of Courses
			Formal Education Courses
			Hiring Practices (i.e. background checks)
	3 <sup>rd</sup> Party Prevention Policies	<i>Third</i>	Business Associate Agreement Signed by 3rd Party
			Ensuring 3rd Party's Plan for Notifying Breach
			Ensuring 3rd Party's Plan for Identifying Breaches
3 <sup>rd</sup> Party HR Policies	<i>eHR</i>	Proof of Employee Training	
		Proof of Employee Background Check	
Auditing	Audit IT Controls	<i>ITAudit</i>	Regular Audit Systems
			IT Audit Logs for Analyzing Inappropriate Access
	Audit Policies	<i>Audit</i>	Specific Policy to Monitor Electronic Health Information
			Regular Audits For Processes Where Patient Info is Shared
			Regular Scheduled Meetings To Review Security Policies
			Process in Place for Reporting Breaches

## Background and Hypotheses

Generally, the goals of information security include regulatory compliance and secure operations (i.e., preventing breaches) (Bulgurcu et al. 2010; Johnston and Hale 2009; Kayworth and Whitten 2010; von Solms 2005;). Weber (1999) suggested that information system controls should be regarded as a system of preventing and auditing illegal events (Weber 1999). Some security research argued that organizations should establish information security systems with preventive control systems and audit systems to reduce security failures (Hong et al. 2003; Straub et al. 2008). These aspects have parallels in quality management where the concept of the cost of quality (COQ) is typically classified into prevention (e.g., design, process engineering), appraisal (e.g., inspection, testing), and internal/external failure costs (e.g., repair) (Behara et al. 2006; Ittner et al. 2001). In addition, conformity to ISO standards has been emphasized as a signal of high quality achievement. Such similarities between information security and quality motivate us to utilize the philosophy of quality management to build our conceptual framework (Naveh, 2004). We categorized a set of information security practices into prevention and audit controls. Further, while information security is perceived to be a technical issue as a low-level technical function, our study tries to examine the importance of information security as a strategic issue by dividing security practices into IT controls and policies. Table 1 lists the categories of such security practices, and Figure 1 describes the conceptual framework.

### Security Prevention and Audit IT Controls

Information security strategy includes a continuous process of identifying and measuring risks, and implementing and monitoring controls (D'Arcy et al. 2009; ITGI 2005). Historically, organizations have followed a technically focused strategy for designing effective security solutions, since information security has been perceived to be a somewhat technical issue (Urbaczewski and Jessup 2002). IT controls are generally believed to improve an organization's ability to monitor suspicious activities and prevent an

information breach. Thus, IT controls increase security performance as well as perceived compliance with regulations. Thus, we hypothesize:

H1a: Security Prevention IT controls are positively associated with perceived regulatory compliance.

H1b: Audit IT controls are positively associated with perceived regulatory compliance.

H1c: Security Prevention IT controls are positively associated with security performance.

H1d: Audit IT controls are positively associated with security performance.

### ***Security Prevention and Audit Policies***

While information security has often been positioned as an independent function from the business, the recent view has started to consider a socio-technical perspective on information security, emphasizing the importance of information security policies when designing and implementing technical solutions. Information security policies contain detailed guidelines for the proper/improper uses of organizational IT resources and security procedures (Puhakainen and Siponen 2010; Siponen and Vance 2010). The policies rely on the same underlying mechanism as societal laws: providing knowledge of what constitutes acceptable and unacceptable conduct increases the efficiency of an organization's security activities through comprehensive information security education of all employees in organizations (Herath and Rao 2009).

H2a: Security Prevention policies are positively associated with perceived regulatory compliance.

H2b: Audit policies are positively associated with perceived regulatory compliance.

H2c: Security Prevention policies are positively associated with security performance.

H2d: Audit policies are positively associated with security performance.

### ***The Balance of Security Prevention and Audit***

For many organizations, auditing all security activities has become as important as ensuring that breach prevention procedures are in place. Von Solms (2005) discussed the differences that should exist between prevention operations and security auditing. He argued that good information security governance can be achieved through a balanced approach, since the two complement each other via shared processes (von Solms 2005). This perspective is also aligned with the concept of COQ that evaluates the optimal trade-offs across prevention and appraisal costs, and the costs of failure. Therefore, we hypothesize:

H3a: The interaction of Security Prevention and Audit IT controls increases perceived regulatory compliance more than either type alone.

H3b: The interaction of Security Prevention and Audit policies increases perceived regulatory compliance more than either type alone.

H3c: The interaction of Security Prevention and Audit IT controls increases security performance more than either type alone.

H3d: The interaction of Security Prevention and Audit policies increases security performance more than either type alone.

### ***Regulatory Compliance and Security Performance***

If an organization complies with internal policies and legal requirements, organizational 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).

H4: The level of an organization's regulatory compliance influences its security performance.

## Data and Research Methodology

We draw data from the Kroll/HIMMS<sup>3</sup> survey of hospitals on patient data safety, conducted in December 2009. This telephone-based survey had a variety of individuals within healthcare organizations that have experience with their organization's privacy and security environment. Respondents included IT executives, Chief Security Officers (CSO), Health Information Management (HIM) Directors, Compliance Officers and Privacy Officers in 250 organizations.

### Dependent Variables

To test the hypotheses, we employ two types of dependent variables: *Compliance* and *Performance*. For *Compliance*, we use a scale of one to seven on compliance with three key regulations: HITECH, HIPAA, and State Security Laws. *Performance* is measured by the number of breach occurrences and by the existence of financial impacts of breaches.

### Independent Variables

Our independent variables include major security practices. The survey provided adoption data on 22 security practices. Among these practices, we selected the practices having significant loadings (>0.5) from a factor analysis, resulting in 8 dimensions. As mentioned before, the security practices were categorized by purpose: ensuring security or auditing. Table 1 shows the assignment of security practices to independent variables.

### Control Variables

Control variables include *Size*, *Type*, *Top level support*, and *Data coordination*. *Size* is measured by the number of licensed beds. *Type* is a dummy variable to describe the organization type. If an organization is a general medical institute, *Type* is set to one; otherwise zero. In addition, we incorporated top-level support for information security and the level of data coordination among departments. These variables control for organizational security maturity. Both variables use a seven-point scale, where seven is highest level of top-level support or coordination (and one is no support or coordination).

#### Level 1

$$Performance_{ij} = Compliance_{0j} + r_{ij} \quad \text{where } r_{ij} \sim N(0, \sigma^2) \quad (1)$$

#### Level 2

$$Compliance_{0j} = \beta_{00} + \beta_{01j}ITPrevention_j + \beta_{02j}ITAudit_j + \beta_{03j}Prevention_j + \beta_{04j}Audit_j + \beta_{05j}ITthird_j + \beta_{06j}third_j + \beta_{07j}(ITPrevention_j \times ITAudit_j) + \beta_{08j}(Prevention_j \times Audit_j) + \beta_{09j}(ITthird_j \times third_j) + \beta_{10j}iHR_j + \beta_{11j}eHR_j + \sum_c \delta_{0cj}Controls_{jc} + u_{0j} \quad (2)$$

where  $u_{0j} \sim N(0, \tau_{00})$

#### Multilevel Model

$$Performance_{ij} = \beta_{00} + \beta_{01j}ITPrevention_j + \beta_{02j}ITAudit_j + \beta_{03j}Prevention_j + \beta_{04j}Audit_j + \beta_{05j}ITthird_j + \beta_{06j}third_j + \beta_{07j}(ITPrevention_j \times ITAudit_j) + \beta_{08j}(Prevention_j \times Audit_j) + \beta_{09j}(ITthird_j \times third_j) + \beta_{10j}iHR_j + \beta_{11j}eHR_j + \sum_c \delta_{0cj}Controls_{jc} + u_{0j} + r_{ij} \quad (3)$$

<sup>3</sup> Kroll is a leader in healthcare data security that has helped some of the largest healthcare providers in the country respond to data security breaches, in partnership with HIMSS, the leading organization representing health information management systems and services.

## Model

The analysis was conducted at two levels using Hierarchical Linear Modeling (HLM), which can trace whether security performance are varying by compliance levels. The HLM estimates an intercept for each compliance level. The following equations express the organization-level,  $Performance_{ij}$  using a pair of linked models: one at the organization level (Level 1) and another at the compliance-level (Level 2). Substituting (1) and (2) yields the multilevel model (3). We first examine the effects of security practices on an organization's compliance status. Then, we investigate the relationship between the adoption of the practices and actual security performance as well as tests how the relationship varies across compliance levels.

## Preliminary Analyses and Results

Table 2 displays the descriptive statistics and inter-correlations between the variables. Note that most correlations are low. Thus, multicollinearity is not a concern in the study. Tables 3 and 4 report the results from the fixed (Equation (2)) and random effect (Equation (3)) models, respectively.

Table 2. Descriptive Statistics and Correlation Matrix

	N	Mean	1	2	3	4	5	6	7	8
1. IT Prevention	250	0.96	1.00							
2.IT Audit	250	0.85	<b>0.29</b>	1.00						
3.3 <sup>rd</sup> Party IT	250	0.79	<b>0.21</b>	<b>0.20</b>	1.00					
4.Data Coordination	250	5.94	0.09	<b>0.26</b>	<b>0.18</b>	1.00				
5. Prevention Policies	250	0.95	<b>0.15</b>	<b>0.20</b>	<b>0.11</b>	0.11	1.00			
6.Audit Policies	250	0.84	<b>0.17</b>	<b>0.55</b>	<b>0.27</b>	<b>0.21</b>	<b>0.23</b>	1.00		
7.3 <sup>rd</sup> Party Prevention Policy	250	0.84	<b>0.14</b>	<b>0.22</b>	<b>0.39</b>	<b>0.25</b>	-0.01	<b>0.32</b>	1.00	
8.HR policy	250	0.90	<b>-0.06</b>	<b>-0.23</b>	<b>-0.25</b>	<b>-0.22</b>	-0.11	<b>-0.23</b>	-0.12	1.00
9.3 <sup>rd</sup> Party HR policy	250	0.57	<b>0.14</b>	<b>0.25</b>	<b>0.42</b>	<b>0.24</b>	<b>0.20</b>	<b>0.21</b>	<b>0.40</b>	<b>-0.22</b>

**Notes.** Bold values are statistically significant correlation coefficients with  $p < 0.05$

The results indicate that none of the IT controls has a significant effect on compliance. H1a and H1b are not supported. On the other hand, auditing policies significantly increase compliance levels for all three regulations ( $\beta_{04}=0.41$  and  $0.38$  in HITECH and HIPAA at  $p < 0.05$ ,  $0.24$  at  $p < 0.10$  in State Laws) supporting H2b, while security policies do not have a significant effect on compliance levels (thus no support for H2a). Likewise, while IT controls do not influence an organization's security performance (no support for H1c and H1d), security policies significantly decrease breach occurrences and the financial impacts of a breach ( $\beta_{03}=-3.36$  and  $-0.40$  at  $p < 0.01$ ), supporting H2c. However, we find no support for H2d (auditing policy).

Although neither IT security or IT audit controls affect compliance and performance, the adoption of both of them significantly decrease breach occurrences and the financial impact of a breach ( $\beta_{07}=-3.36$  and  $-0.40$  at  $p < 0.01$ ), as well as increase compliance in state laws ( $\beta_{07}=0.92$  at  $p < 0.10$  in HIPAA and  $\beta_{07}=0.30$  at  $p < 0.01$  in state laws). Thus, H3a and H3c are supported. In terms of policies, the interaction of security and audit policies also improve compliance levels ( $\beta_{08}=2.10$  in HITECH at  $p < 0.05$ ) and security performance by preventing breach occurrence and financial impacts ( $\beta_{08}=-13.84$  and  $-1.11$  at  $p < 0.01$ ). These results support H3b and H3d. When the effects of security practices are separately tested against information breaches (from both the inside and outside the organization), internal breaches significantly decline ( $\beta_{08}=-1.28$  at  $p < 0.01$ ) more than external breaches ( $\beta_{08}=-0.42$  at  $p < 0.05$ ).

We further investigate whether security performance differs with compliance levels. Although we have tested all three regulations, we have reported only HITECH compliance for a random effect, since HITECH has the most representative effect among the regulations. Table 4 shows the estimates for the random effects of the model. The results show the estimate values of  $\tau_{00} = 0.03$  and  $\sigma^2 = 3.21$ . The  $p$  values of hypothesis tests indicate that the variance among HITECH compliance levels is not significant but the variance among organizations with their own security practices is significant. Thus, we can suggest that an organization's security performance does not vary with their belief about its compliance, but vary with its security practices. Therefore, an organization's security performance depends on its security practices, not its perception of compliance level.

	Model(1)			Model(2)		
	HITECH	HIPAA	State Laws	HITECH	HIPAA	State Laws
IT Prevention	0.39 (0.36)	0.02 (0.26)	0.28 (0.29)	0.42 (0.36)	0.06 (0.20)	0.28 (0.28)
IT Audit	0.04 (0.19)	-0.12 (0.13)	0.18 (0.15)	-0.01 (0.19)	-0.08 (0.11)	0.18 (0.15)
3 <sup>rd</sup> Party IT	0.11 (0.13)	-0.04 (0.09)	0.13 (0.10)	0.11 (0.13)	0.04 (0.08)	0.13 (0.11)
Prevention Policies	-0.17 (0.28)	-0.18 (0.20)	-0.16 (0.23)	-0.14 (0.28)	0.04 (0.09)	-0.15 (0.22)
Audit Policies	0.45* (0.24)	0.41** (0.17)	0.24 (0.19)	0.41** (0.21)	0.38** (0.14)	0.24* (0.20)
3 <sup>rd</sup> Party Prevention Policy	0.17 (0.19)	0.06 (0.14)	0.10 (0.15)	0.18 (0.19)	0.18 (0.11)	0.08 (0.19)
HR policy	0.06 (0.37)	0.11 (0.27)	0.04 (0.29)	0.44* (0.23)	0.02 (0.05)	0.11 (0.09)
3 <sup>rd</sup> Party HR policy	-0.65 (0.61)	-0.15 (0.47)	0.02 (0.49)	0.26** (0.12)	0.06* (0.03)	0.114 (0.09)
Data Coordination	0.10** (0.04)	0.15*** (0.04)	0.14*** (0.04)	0.10** (0.05)	0.14*** (0.03)	0.15*** (0.04)
<b>Interaction Effects</b>						
IT Prevention × IT Audit	-	-	-	1.32 (0.93)	0.92* (0.49)	0.30*** (0.12)
Prevention × Audit Policies	-	-	-	2.10** (1.05)	0.11 (0.08)	0.11 (0.09)
3 <sup>rd</sup> Party IT × 3 <sup>rd</sup> Party Prevention Policy	-	-	-	0.08** (0.04)	0.07*** (0.02)	0.09*** (0.03)
<b>Controls</b>						
Top level Support	0.09* (0.4)	0.08** (0.03)	0.04 (0.03)	0.12*** (0.04)	0.09*** (0.03)	0.04 (0.04)
size	0.01 (0.07)	0.07 (0.05)	0.14 (0.06)	0.00 (0.07)	0.06 (0.05)	0.12** (0.05)
General Medical	-0.25** (0.10)	-0.03 (0.07)	-0.09 (0.08)	-0.23*** (0.09)	-0.024 (0.08)	-0.92 (0.08)
<b>Adj R-Square</b>	0.24	0.20	0.24	0.25	0.20	0.24

**Notes.** Standard errors are in parentheses.  $p$ -values are represented by \* Significant at  $p < 0.10$ , \*\* Significant at  $p < 0.05$ , \*\*\* Significant at  $p < 0.01$ .

## Conclusions

This study examines how a healthcare organization's security practices (including IT controls, policies, education, and hiring practices) influence managers' perceived 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. Healthcare organizations must focus on preventing breaches (which results in brand damage and direct remediation costs) as well as complying with government regulation (to avoid

indirect costs, including fines and penalties). We categorized security practices into security and auditing strategies.

	Model(1)				Model(2)			
	Breach#	Inside	Outside	Financial Impacts	Breach#	Inside	Outside	Financial Impacts
IT Prevention	0.71 (1.08)	0.17 (0.15)	0.07 (0.07)	-0.02 (0.09)	4.61** (1.92)	0.41* (0.28)	0.19 (0.13)	0.29* (0.17)
IT Audit	0.16 (0.56)	0.07 (0.08)	-0.06* (0.03)	0.03 (0.05)	4.11* (2.53)	0.36 (0.38)	0.06 (0.17)	0.37* (0.22)
3 <sup>rd</sup> Party IT	0.25 (9.41)	0.01 (0.05)	0.00 (0.03)	0.04 (0.03)	-0.17 (0.91)	-0.02 (0.13)	-0.01 (0.06)	0.01 (0.07)
Prevention Policies	-3.36*** (0.85)	-0.40*** (0.12)	-0.07 (0.05)	-0.22*** (0.07)	6.60** (2.33)	0.52 (0.34)	0.23 (0.15)	0.57** (0.20)
Audit Policies	0.42 (0.75)	0.06 (0.10)	0.07 (0.04)	0.05 (0.06)	13.15*** (2.94)	1.27*** (0.44)	0.46** (0.20)	1.07*** (0.26)
3 <sup>rd</sup> Party Prevention Policy	0.36 (0.62)	0.03 (0.08)	0.05 (0.04)	-0.07 (0.05)	0.12 (0.96)	-0.03 (0.13)	0.04 (0.06)	0.05 (0.08)
HR policy	-1.94** (0.78)	-0.28**** (0.10)	-0.06 (0.04)	-0.04 (0.06)	1.88 (1.75)	0.26 (0.20)	0.06 (0.05)	0.03 (0.06)
3 <sup>rd</sup> Party HR policy	-0.67* (0.36)	-0.08 (0.05)	-0.01 (0.02)	-0.06* (0.03)	-0.61* (0.35)	-0.08* (0.05)	-0.01 (0.02)	-0.06** (0.03)
Data Coordination	0.06 (0.15)	-0.02 (0.2)	-0.02* (0.01)	-0.00 (0.01)	0.09 (0.144)	-0.01 (0.02)	-0.02* (0.01)	-0.00 (0.01)
<b>Interaction Effects</b>								
IT Prevention × IT Audit	-	-	-	-	-4.95* (2.72)	-0.35 (0.40)	-0.15 (0.18)	-0.40* (0.23)
Prevention × Audit Policies	-	-	-	-	-13.84*** (3.07)	-1.28*** (0.45)	-0.42** (0.20)	-1.11*** (0.27)
3 <sup>rd</sup> Party IT × 3 <sup>rd</sup> Party Prevention Policy	-	-	-	-	0.15 (0.39)	0.02 (0.05)	0.01 (0.02)	0.01 (0.03)
<b>Controls</b>								
Top level Support	-0.16 (0.15)	-0.00 (0.20)	-0.00 (0.01)	-0.00 (0.01)	-0.09 (0.15)	0.00 (0.02)	-0.00 (0.01)	0.00 (0.01)
size	0.78 (0.23)	0.07** (0.03)	0.05 (0.01)	0.09*** (0.02)	0.68*** (0.23)	0.06 (0.03)	0.05*** (0.01)	0.08*** (0.018)
General Medical	-0.41 (0.33)	-0.04 (0.04)	-0.05 (0.02)	-0.08*** (0.03)	-0.46 (0.31)	-0.04 (0.05)	-0.06*** (0.02)	-0.09*** (0.026)
<b>Random Effects</b>								
Intercept(HITECH)	0.05 (0.12)	0.00 (0.00)	0.00 (0.00)	0.00 (0.00)	0.03 (0.08)	0.00 (0.00)	0.00 (0.00)	0.00 (0.00)
Residual	3.21*** (0.35)	0.07*** (0.01)	0.01*** (0.00)	0.02*** (0.00)	3.10*** (0.34)	0.06*** (0.01)	0.01*** (0.00)	0.02*** (0.00)
<b>Adj R-Square</b>	0.19	0.14	0.12	0.19	0.25	0.14	0.15	0.23

**Notes.** Standard errors are in parentheses. *p*-values are represented by \* Significant at  $p < 0.10$ , \*\* Significant at  $p < 0.05$ , \*\*\* Significant at  $p < 0.01$ .

Using the HLM, we examined the effects of the practices on security performance and regulatory compliance. We also investigated whether the level of compliance actually affects security performance. The results show that audit policies are positively associated with perceived regulatory compliance and security policies are associated with security performance. Further, we find that the interaction of both audit and security policies has a more significant effect than that of either type of the controls alone. Surprisingly, an organization's level of perceived compliance is not significantly associated with actual security performance.

We draw important implications from these findings. Given that existing regulations allow for varying applications and interpretations of compliance, healthcare organizations have evaluated compliance levels according to the adopted auditing policies. However, our results imply that the organization's perception of compliance had little impact on actual security performance. Therefore, policy makers should focus on providing incentives for security investment rather than solely depending on compliance. We also conclude that the combined impact of security operations and auditing strategies is better than that of either alone. Thus, organizations that balance investment between security operations and auditing, improve both compliance and security performance.

## References

- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), Sep 2010, pp 523-548.
- D'Arcy, J., Hovav, A., and Galletta, D. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1) 2009, pp 79-98.
- Garfinkel, R., Gopal, R., and Thompson, S. "Releasing individually identifiable microdata with privacy protection against Stochastic threat: An application to health information," *Information Systems Research* (18:1) 2007, pp 23-41.
- Herath, T., and Rao, H.R. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), Apr 2009, pp 106-125.
- Hong, K., Chi, Y., Chag, L.R., and Tang, J. "An Integrated System Theory of Information Security Management," *Information Management & Computer Security* (11:5) 2003, p 243.
- Ittner, C.D., Nagar, V., and Rajan, M.V. 2001."An Empirical Examination of Dynamic Quality-based Learning Models," *Management Science* (47:4), April, pp. 563-578.
- ITGI "Board Briefing on IT Governance," <http://www.isaca.org/sox/>, 2005.
- Johnston, A.C., and Hale, R. "Improved Security through Information Security Governance," *Communications of the ACM* (52:1) 2009, pp 126-129.
- Johnston, A.C., and Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), Sep 2010, pp 549-566.
- Kayworth, T., and Whitten, D. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive* (9:3), Sep 2010, pp 163-175.
- Liberti, L. "Survey Results: Reduce the Cost of Compliance While Strengthening Security," in: *Security Management Newsletter*, 2008.
- McFadzean, E., Ezingear, J.N., and Birchall, D. "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Information Review* (31) 2007, pp 622-660.
- Puhakainen, P., and Siponen, M. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), Dec 2010, pp 757-778.
- Siponen, M., and Vance, A. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), Sep 2010, pp 487-502.
- Spears, J.L., and Barki, H. "User Participation In Information Systems Security Risk Management," *MIS Quarterly* (34:3), Sep 2010, pp 503-522.
- Straub, D.W., Goodman, S.E., and Baskerville, R. *Information security: policy, processes, and practices* M.E. Sharpe, 2008.
- Straub, D.W., and Nance, W.D. "Discovering and Disciplining Computer Abuse in Organizaitons - A Field-Study," *MIS Quarterly* (14:1), Mar 1990, pp 45-60.
- Urbaczewski, A., and Jessup, L.M. "Does electronic monitoring of employee Internet usage work?," *Communications of the ACM* (45:1), Jan 2002, pp 80-83.
- von Solms, S.H. "Information Security Governance - Compliance management vs operational management," *Computers & Security* (24:6) 2005, pp 443-447.
- Weber, R. *Information System Control and Audit* Prentice-Hall, 1999.