Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings

Proceedings

Security Practices and Regulatory Compliance in the Healthcare Industry

Juhee Kwon
Tuck School of Business, Dartmouth College, Hanover, NH, United States., juhee.kwon@dartmouth.edu

M. Eric Johnson
Tuck School of Business, Dartmouth College, Hanover, NH, United States., m.eric.johnson@dartmouth.edu

Security Practices and Regulatory Compliance in the Healthcare Industry[*]

Juhee Kwon
Tuck School of Business
Dartmouth College, Hanover, NH 03755
juhee.kwon@dartmouth.edu

M. Eric Johnson
Tuck School of Business
Dartmouth College, Hanover, NH 03755
m.eric.johnson@dartmouth.edu

ABSTRACT

This study examined the adoption of security practices, with the goal of identifying dominant configurations and their relationship to perceived compliance. We utilized survey data from 204 hospitals including adoption status of 17 security practices and perceived compliance levels on HITECH, HIPAA, Red Flags Rules, CMS, and State laws governing patient information security. Using cluster analysis and t-tests, we found that three clusters of security practices are significantly associated with different levels of perceived compliance. We demonstrated significant differences among non-technical practices rather than technical practices, and the highest levels of compliance are associated with hospitals that employed a balanced approach between technical and non-technical practices (or between one-time and cultural practices). Our results provide security practice benchmarks for healthcare administrators and can help policy makers in developing strategic and practical guidelines for practice adoption.

Keywords

Security Practices, Compliance, Healthcare, Regulation.

INTRODUCTION

Growing concern over protected healthcare information security in the U.S. has led to increased regulation and changes in the required security practices needed to achieve compliance. However, some surveys by both industry groups and the US Department of Health and Human Services (HHS) noted wide disparity both in security practices and in perceived compliance with federal (HITECH/HIPAA) and state regulations (HHS 2005; Pavolotsky 2011). It is not surprising that hospital practices vary, given the heterogeneity of federal and state regulation. However, low levels of perceived compliance indicate that managers are uncertain about their own practices and the required path to compliance.

Given the variety of security practices that hospitals can implement, how do managers make strategic implementation choices? How are different sets of security practices associated with perceived regulatory compliance? Although recent research has paid attention to the organizational and the socio-technical aspects of security management (Johnston and Warkentin 2010; Kayworth and Whitten 2010), there is a dearth of empirical literature that considers the relationship between the configuration of security practices and perceived compliance. This paper represents one effort at addressing this void in the informatics literature by providing a snapshot of security practices and regulatory compliance.

Through our analysis using clustering and then comparing those clusters via t-tests, we identified three clusters of security practices that are associated with different levels of perceived regulatory compliance. Although high practice adoption, across the board, was generally associated with high compliance, our analysis revealed patterns of practice and compliance. We found that audit practices were important to those who scored in the middle of the pack on compliance. However, hospitals in the highest cluster of compliance were also significantly managing third-party breaches and training. Our results provide security practice benchmarks for healthcare administrators and can help policy makers in developing strategic and practical guidelines for practice adoption.

[*] *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)*

The reminder of this paper is organized as follows. The next section provides research background on security and compliance from prior literature. Then, we describe our data and the research methods followed by the results. The paper concludes with a discussion of our findings and their implications for practice and future research.

BACKGROUND

Security practices include management processes for detecting and mitigating risks as well as the implementation of technical safeguards (ITGI 2005; D'Arcy et al. 2009). Unfortunately, many healthcare organizations follow a reactive path of implementing technical stopgaps because information security has been perceived to be largely a technical issue—independent from the business of providing care (Urbaczewski and Jessup 2002; Murphy et al. 2011). However, that view is beginning to shift towards a more holistic socio-technical perspective on information security, emphasizing the importance of integrating technical solutions with organizational security culture, policies, and education (Collmann and Cooper 2007; Puhakainen and Siponen 2010; Siponen and Vance 2010). A socio-technical perspective relies on many of the same underlying mechanisms as societal laws: providing knowledge (through education) of what constitutes acceptable and unacceptable conduct to increase the efficiency of an organization's security activities (Herath and Rao 2009).

Given the heterogeneity of security practices, researchers and practitioners have called for organizations to be more strategic in their approach to information security—yet it has not always been clear what such an approach looks like in practice (Johnston and Warkentin 2010; Kayworth and Whitten 2010; Spears and Barki 2010). Organizations are faced with a dynamic information security environment characterized by constantly changing risks and legal compliance issues (Beard et al. 2012). Within this environment, healthcare organizations must develop a security strategy that both ensures compliance as well as protects patient information. Organizations that achieve this objective will have a highly effective information security strategy. However, many have emphasized simple checklists of technical components rather than striving to deploy strategic solutions (Puhakainen and Siponen 2010). Therefore, this study attempts to provide better strategic implementation choices for hospitals by identifying the relationship between security practices and regulatory compliance.

RESEARCH METHODOLOGY

Data Source and Sampling

We utilized data from the Kroll/HIMMS[†] hospital survey, which was designed to examine effective patient data security practices and management measures. The survey data includes responses from 250 hospitals, including adoption of 17 different security practices (1 if adopted, 0 otherwise) and perceived levels of regulatory compliance for HITECH, Red Flag Rules, HIPAA, State laws, and CMS regulations (measured on a seven-point scale where 1 is "not at all compliant" and 7 is "compliant with all applicable standards"). We also included organizational variables, which are commonly used in health economics to control for the size and type of organization. In our model, *size* is the number of licensed beds (measured on a three-point scale where 1 is under 100 beds, 2 is 100 to 299 beds, and 3 is 300 beds or more) and *critical access, general medical,* and *academic* are all (exclusive) dummy variables that describe the hospital type. Table 1 provides descriptive statistics for the variables in our analysis.

Among the 250 observations, 46 hospitals were dropped because of missing data, and thus our final sample included 204 hospitals. Our analysis considered the relationship between individual security practices and compliance, categorizing practices into those that involve safeguarding information, auditing, HR management, and third party management. Table 1 provides descriptive statistics for the variables in our analysis.

Cluster Analysis

Table 2 provides the correlations between security practices. Although several practices were highly correlated within the different domains (i.e., safeguarding information, auditing, HR management, and third party management), the security practices each have specific data protection features. Thus, we retained all 17 practices for cluster analysis.

[†] *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.*

Variable Name	Description (dichotomous indicators unless noted)	Mean	Std Dev	Min	Max
Safeguarding Information					
IT Sec	Technical IT Security Measures (i.e. firewalls, encrypted e-mails, network monitoring, intrusion detection etc.)	0.98	0.14	0.00	1.00
Report Breaches	Process in Place for Reporting Breaches In Patient Information	0.97	0.17	0.00	1.00
Data Access	Data Access Minimization (i.e. giving employees only the information they need)	0.94	0.24	0.00	1.00
Who They Say They Are	Ensuring that Patient Is Who They Say They Are	0.91	0.28	0.00	1.00
Access & Sharing Policies	Specific Policy in place to Monitor Electronic Patient Health Information Access and Sharing	0.87	0.33	0.00	1.00
Auditing					
IT Audit	IT Applications Have Audit Functions that monitor the access and use of patient information	0.95	0.22	0.00	1.00
Audit Systems	Regular Audits Are Conducted of Systems That Generate/Collect/Transmit Patient Data	0.87	0.33	0.00	1.00
Audit IT logs	IT Audit Logs Are Created and Analyzed For Inappropriate Access to Patient Data	0.83	0.37	0.00	1.00
Audit policies	Regular Scheduled Meetings Are Conducted To Review Status of Data Security Policies	0.77	0.42	0.00	1.00
Audit shared data	Regular Audits Are Conducted For Processes Where Patient Info is Shared with External Orgs	0.74	0.44	0.00	1.00
HR Management					
Hiring Practices	Hiring Practices (i.e. background checks)	0.97	0.17	0.00	1.00
HR monitor	Human Resources monitors completion of courses on confidential patient data for hiring and continuing education tasks	0.88	0.32	0.00	1.00
Education	Formal Education Courses	0.86	0.35	0.00	1.00
Third Party Management					
Third-party Agreement	Business Associate Agreement Signed by third-party	0.98	0.14	0.00	1.00
Report third-party breaches	Proof of Employee Training	0.79	0.41	0.00	1.00
Detect third-party breaches	Ensure that third-party Has Plan for Notifying Covered Entities of Breach	0.76	0.43	0.00	1.00
Third-party Training	Ensure that third-party Has Plan for Identifying Breaches	0.61	0.49	0.00	1.00
Compliance (1 - “not at all compliant”, 7 - “compliant with all applicable standards)					
HITECH	HITECH	5.75	1.39	1.00	7.00
Red	Red flags Rule	6.14	1.21	1.00	7.00
HIPAA	HIPAA	6.59	0.70	2.00	7.00
State	State Security Laws	6.38	0.97	1.00	7.00
CMS	CMS Regulations	6.61	0.65	4.00	7.00
Organizational Information (Control Variables)					
Size	Size (1 - 100, 2 - 100 to 299, 3 - 300+ beds)	1.63	0.71	1.00	3.00
Critical Access	Critical Access	0.35	0.48	0.00	1.00
General Med	General Med/Surg	0.55	0.50	0.00	1.00
Academic	Academic	0.04	0.19	0.00	1.00

Table 1 Descriptive Statistics

		1)	2)	3)	4)	5)	6)	7)	8)	9)	10)	11)	12)	13)	14)	15)	16)	17)	18)	19)	20)	21)
Safeguarding Information	1) IT Sec	1																				
	2) Report Breaches	-0.02	1																			
	3) Data Access	**0.27**	-0.04	1																		
	4) Who They Say They Are	0.08	**0.25**	0.07	1																	
	5) Access & Sharing Policies	0.05	0.11	**0.15**	**0.14**	1																
Auditing	6) IT Audit	**0.13**	-0.04	**0.33**	0.01	**0.39**	1															
	7) Audit Systems	0.05	**0.28**	**0.22**	**0.24**	**0.34**	**0.19**	1														
	8) Audit IT logs	**0.13**	**0.16**	0.06	**0.19**	**0.22**	**0.26**	**0.38**	1													
	9) Audit policies	0.01	**0.25**	0.01	**0.28**	**0.21**	-0.07	**0.31**	**0.19**	1												
	10) Audit shared data	0	**0.29**	0.09	**0.21**	**0.17**	0.12	**0.47**	**0.36**	**0.31**	1											
HR	11) Hiring Practices	-0.02	-0.03	0.08	-0.05	0.02	0.09	-0.07	0.08	-0.03	-0.04	1										
	12) HR monitor	-0.05	**0.21**	-0.03	**0.15**	0.00	-0.08	**0.18**	0.04	**0.16**	**0.16**	**0.21**	1									
	13) Education	0.04	0.1	**0.14**	**0.17**	0.01	-0.03	**0.22**	**0.19**	**0.21**	**0.3**	0.1	**0.2**	1								
Third Party	14)Third-party Agreement	-0.02	-0.02	-0.04	-0.04	-0.05	-0.03	-0.05	-0.06	0.09	0.00	-0.02	-0.05	0.04	1							
	15)Report third-party breaches	0.02	**0.2**	0.08	0.06	0.10	0.11	**0.24**	**0.23**	**0.24**	**0.27**	-0.02	**0.12**	**0.14**	**0.19**	1						
	16)Detect third-party breaches	0	**0.17**	**0.15**	0.03	0.13	**0.14**	**0.16**	**0.18**	**0.26**	**0.29**	0.04	**0.12**	0.07	**0.17**	**0.74**	1					
	17)Third-party Training	0.03	**0.16**	**0.14**	**0.17**	0.08	**0.14**	**0.17**	**0.26**	0.11	**0.25**	0.04	0.08	**0.19**	**0.18**	**0.39**	**0.39**	**1**				
Regulations	18) HITECH	0.00	0.11	**0.16**	0.06	**0.20**	0.16	**0.23**	**0.16**	**0.25**	**0.15**	**0.23**	**0.28**	-0.01	-0.03	**0.31**	**0.35**	**0.32**	1			
	19) RED	-0.07	**0.21**	**0.15**	**0.17**	0.09	0.03	**0.14**	0.10	**0.25**	**0.16**	**0.15**	**0.14**	0.12	**0.16**	**0.19**	**0.19**	**0.19**	**0.45**	1		
	20) HIPAA	0.02	**0.15**	0.09	0.01	0.09	**0.16**	**0.20**	**0.15**	**0.22**	**0.18**	**0.16**	0.07	0.02	0.02	**0.27**	**0.23**	**0.26**	**0.44**	**0.29**	1	
	21) State	0.06	**0.16**	**0.16**	0.12	0.14	**0.16**	**0.20**	**0.22**	**0.26**	**0.16**	**0.26**	0.08	0.01	-0.02	**0.24**	**0.26**	**0.33**	**0.39**	**0.34**	**0.57**	1
	22) CMS	0.08	0.07	0.11	0.13	**0.22**	0.11	0.13	**0.22**	**0.36**	**0.28**	**0.25**	**0.15**	-0.06	0.02	**0.21**	**0.24**	**0.30**	**0.45**	**0.35**	**0.45**	**0.55**

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

Table 2 Correlations among Security Practices and Regulatory Compliance

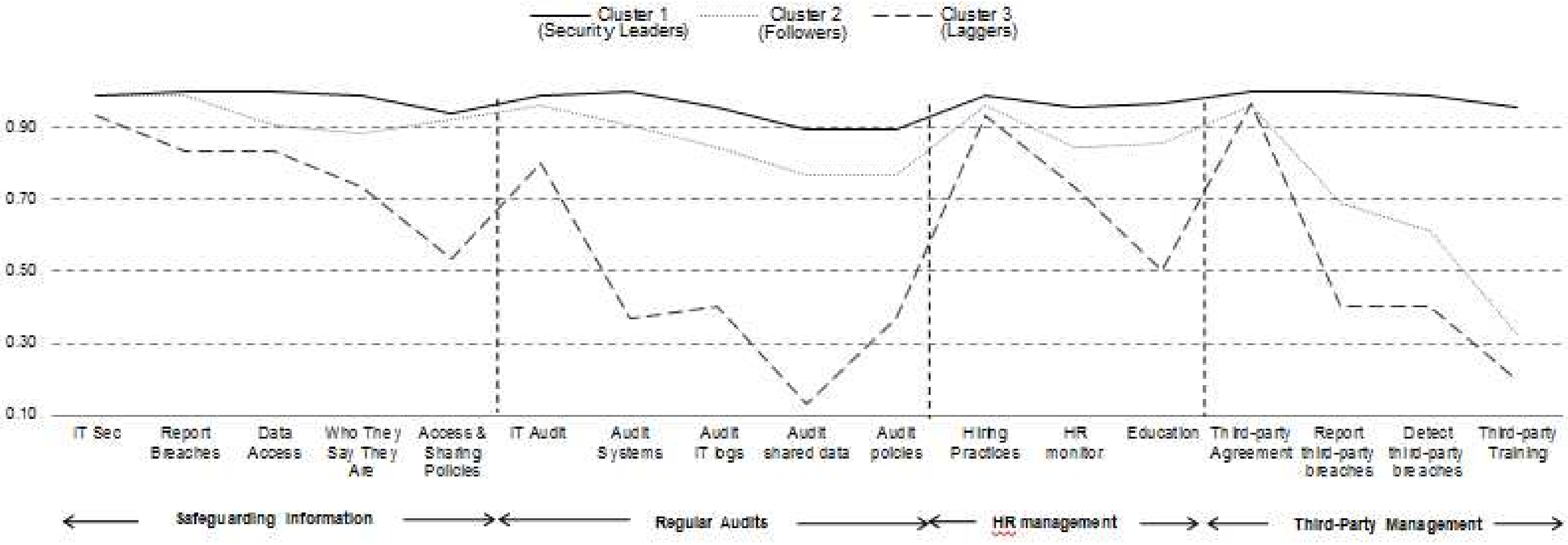


Figure 1 Security Management Clusters (average practice adoption for each cluster)

To derive distinct and meaningful configurations from the security practices, we employed cluster analysis using distance measures based on response pattern similarity. In various contexts, such as psychological testing and marketing, cluster analysis has been found to be a useful means for exploring datasets and identifying underlying groups among individuals (Ravichandran and Rai 1999; Ferratt et al. 2005). In this study, we employed cluster analysis to examine groups of association among security practices. We employed Ward's clustering algorithm (minimum-variance method), which calculates distance between hospitals using dichotomous data indicating the presence or absence of security practices.

With the result from clustering, we then examined three statistical criteria in order to ensure the reliability of the appropriate number of clusters: cubic clustering criterion, pseudo-F, and pseudo-T2 (Milligan and Cooper 1985). Local peaks of the cubic clustering criterion and pseudo-F combined with a small value of the pseudo-T2 (11.6) led us to conclude that the most appropriate number of clusters was three. In addition, a large pseudo-T2 (189) of the next cluster solution (4) suggests that a good solution occurred immediately prior (3) (Institute 1990).

We further tested the validity of the clusters using discriminant analysis, which is often used to verify the results of cluster analysis. The analysis runs the training data back through the minimum-variance method as a discriminant function to see how accurately they are classified. The results from our analysis indicated high levels of classification accuracy (95.88%, 80.52%, and 93.33% for clusters 1, 2, and 3, respectively). Appendix E provides details this analysis.

RESULTS

Clusters of Security Practices

Through Ward's clustering, three statistical criteria and discriminant analysis, we found that the hospitals' security practice adoption patterns could be classified into three clusters. As shown in Table 3, cluster 1 are the security leaders, with the highest levels of security-practice adoption, cluster 2 are close followers with the second highest level, and cluster 3 are the laggers with the lowest level. The security leaders in cluster 1 and the close followers in cluster 2 consist primarily of general medical organizations, 60% and 57% respectively, followed by critical access and academic institutes. On the other hand, the laggers in cluster 3 consist of critical access (63%) and general medical organizations (33%), but no academic institutes. In terms of size, the laggers (1.33) are significantly smaller than the security leaders (1.67) and followers (1.69). This may imply that the laggers' low adoption is attributed to the limited budgets of relatively small hospitals.

Figure 1 visually describes the clusters using the mean values of the security practices provided in Table 3. It reveals interesting patterns of security practices. The security leaders in cluster 1 show high adoption across all practices while the others have big gaps. First, note that adoption of technical solutions for safeguarding information are not significantly different (from 0.93 to 0.99) among three clusters. IT audit applications also have smaller differences (0.80 to 0.99), with the notable exception of non-technical audit practices (from 0.13 to 1.00). However, the figure shows that there was wide variation in adoption of non-technical practices like policies and procedures. For instance, the adoption of accessing & sharing policies ranges from 0.53 to 0.94, and the adoption of shared data audits ranges from 0.13 to 0.90.

Second, we can see that hospitals gave more weight to safeguarding information than to preforming regular audits. All three clusters have higher mean values for safeguarding (0.98, 0.94, and 0.77 for the security leaders, followers and laggers, respectively) than auditing (0.95, 0.85, and 0.41). Furthermore, the standard deviations for safeguarding information are smaller than for auditing (0.09, 0.22, and 0.39 vs. 0.18, 0.34, and 0.45). This indicates that the adoption of safeguarding practices have less differences among hospitals than those of audit practices (for all clusters).

Third, in terms of HR management, most of hospitals have adopted one-off practices such as background checking in hiring (0.99, 0.96, and 0.93). On the other hand, their adoption of cultural practices such as continuous monitoring (0.96, 0.84, and 0.74) and employee education (0.97, 0.86, and 0.50) varies.

Lastly, we see big differences between the three clusters for third-party management—the followers (cluster 2) and laggers (cluster 3) depended more on agreements signed by third parties than on implementing actual practices like third-party breach management or training. While 97% of the laggers had third-party agreements, only 20% had adopted third-party training programs and 40% had third-party breach management. On the other hand, 96% of the security leaders (cluster 1) had training programs and more than 99% had other third-party practices.

Clusters	Cluster 1 (Leaders) (n=97)		Cluster 2 (Followers) (n=77)		Cluster 3 (Laggers) (n=30)		1-2	1-3	2-3
Variable Name	Mean	Std Dev	Mean	Std Dev	Mean	Std Dev	*Mean Difference*		
Safeguarding Information									
IT Sec	0.99	0.10	0.99	0.11	0.93	0.25	0.00	0.06	0.06
Report Breaches	1.00	0.00	0.99	0.11	0.83	0.38	0.01	0.17**	0.16**
Data Access	1.00	0.00	0.91	0.29	0.83	0.38	0.09**	0.17**	0.08
Who They Say They Are	0.99	0.10	0.88	0.32	0.73	0.45	0.11**	0.26***	0.15*
Access & Sharing Policies	0.94	0.24	0.92	0.27	0.53	0.51	0.02	0.41***	0.39***
Domain Mean	***0.98***	***0.09***	***0.94***	***0.22***	***0.77***	***0.39***	***0.05***	***0.21***	***0.17***
Auditing									
IT Audit	0.99	0.10	0.96	0.19	0.80	0.41	0.03	0.19**	0.16**
Audit Systems	1.00	0.00	0.91	0.29	0.37	0.49	0.09**	0.63***	0.54***
Audit IT logs	0.96	0.20	0.84	0.37	0.40	0.50	0.12**	0.56***	0.44***
Audit policies	0.90	0.31	0.77	0.43	0.37	0.49	0.13**	0.53***	0.4***
Audit shared data	0.90	0.31	0.77	0.43	0.13	0.35	0.13**	0.77***	0.64***
Domain Mean	***0.95***	***0.18***	***0.85***	***0.34***	***0.41***	***0.45***	***0.10***	***0.54***	***0.44***
HR Management									
Hiring Practices	0.99	0.10	0.96	0.19	0.93	0.25	0.03	0.06	0.03
HR monitor	0.96	0.20	0.84	0.37	0.73	0.45	0.12**	0.23**	0.11
Education	0.97	0.17	0.86	0.35	0.50	0.51	0.11**	0.47***	0.36**
Domain Mean	***0.97***	***0.16***	***0.89***	***0.30***	***0.72***	***0.40***	***0.09***	***0.25***	***0.17***
Third Party Management									
Third-party Agreement	1.00	0.00	0.96	0.19	0.97	0.18	0.04	0.03	-0.01
Report third-party breaches	1.00	0.00	0.69	0.47	0.40	0.50	0.31***	0.60***	0.29**
Detect third-party breaches	0.99	0.10	0.61	0.49	0.40	0.50	0.38***	0.59***	0.21*
Third-party Training	0.96	0.20	0.32	0.47	0.20	0.41	0.64***	0.76***	0.12
Domain Mean	***0.99***	***0.08***	***0.65***	***0.41***	***0.49***	***0.40***	***0.34***	***0.50***	***0.15***
Grand Mean	***0.97***	***0.13***	***0.83***	***0.31***	***0.59***	***0.41***	***0.14***	***0.37***	***0.23***
Compliance									
HITECH	6.35	1.07	5.38	1.31	4.73	1.60	0.97***	1.62***	0.65**
Red	6.59	0.75	5.74	1.45	5.73	1.23	0.85***	0.86***	0.01
HIPAA	6.77	0.47	6.52	0.79	6.17	0.87	0.25**	0.6***	0.35
State	6.71	0.59	6.25	1.00	5.67	1.37	0.46***	1.04***	0.58**
CMS	6.85	0.39	6.53	0.66	6.03	0.89	0.32***	0.82***	0.5**
	6.65	***0.65***	***6.08***	***1.04***	***5.67***	***1.19***	***0.57***	***0.99***	***0.42***
Organizational Information									
Size	1.67	0.69	1.69	0.75	1.33	0.61	-0.02	0.34**	0.36**
Critical Access	0.29	0.46	0.32	0.47	0.63	0.49	-0.03	-0.34***	-0.31**
General Med	0.60	0.49	0.57	0.50	0.33	0.48	0.03	0.27**	0.24**
Academic	0.04	0.20	0.05	0.22	0.00	0.00	-0.01	0.04**	0.05**

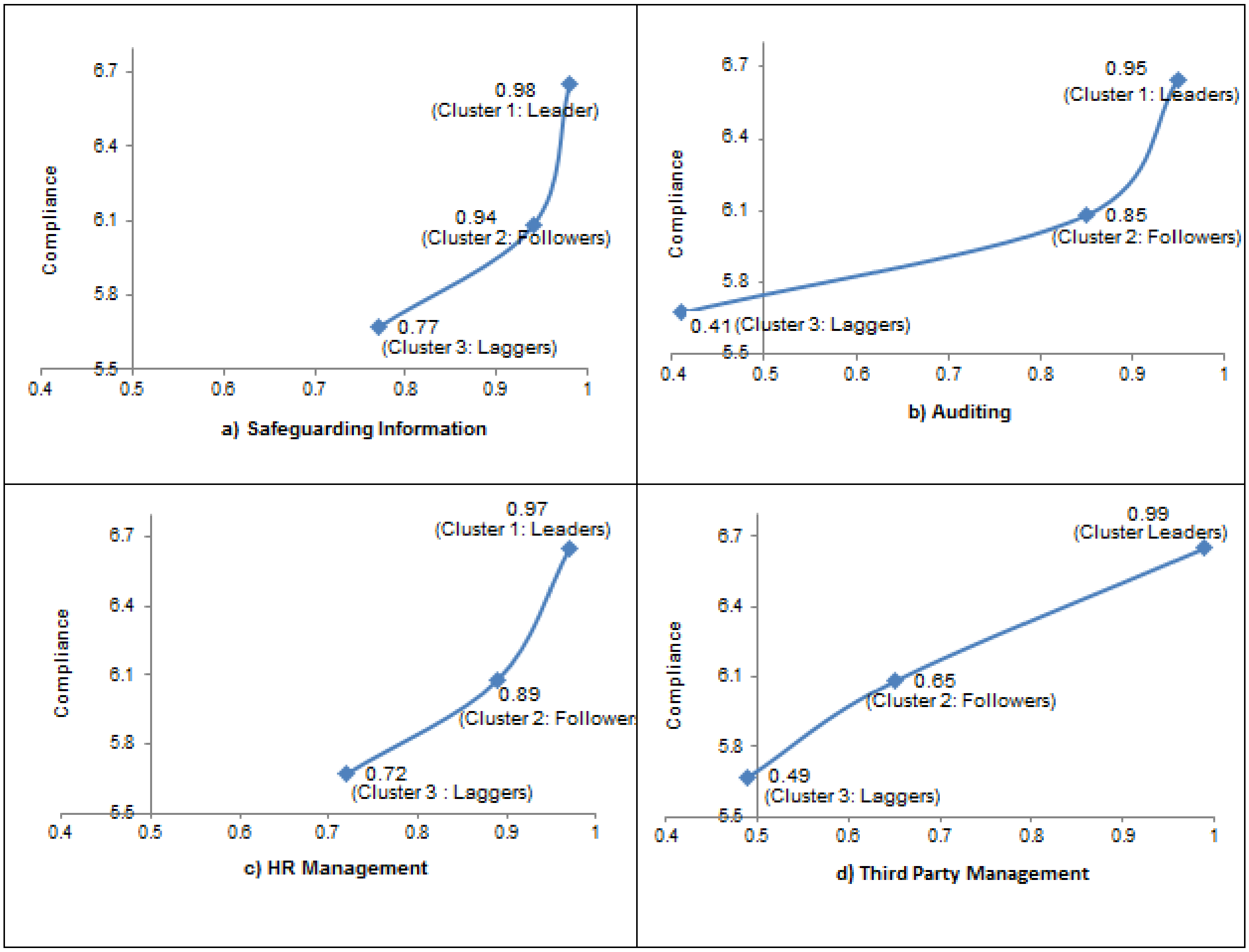
Notes. *p-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at p <0.01. Values in bold represent the average values of each domain.*

Table 3 Clustering Security Practices

Security Practices and Regulatory Compliance

We further investigated (with t-tests) the relationship between the three clusters and perceived regulatory compliance. The comparisons allowed us to test how the adoption levels of security practices are associated with perceived regulatory compliance. Figure 2 describes the relationships between three clusters' practice adoption and regulatory compliance for each of the four security domains. The graphs indicate that the effects of security practices are not uniform across the clusters as well as the security domains. First, the adoption levels within safeguarding (0.77 to 0.98) and HR practices (0.72 to 0.97) are not significantly distinguished among the security leaders, followers and laggers (see Table 3). This indicates that the followers and laggers already reached solid adoption levels within these domains.

On the other hand, the adoption levels within auditing (0.41 to 0.95) and third party practices (0.49 to 0.99) are widely dispersed across the three clusters. While the auditing distance between the security leaders in cluster 1 and the followers in cluster 2 is close, the laggers in cluster 3 significantly fell below the followers as shown in Table 3. In particular, regular audit policies and procedures have significantly larger differences than IT audit application. That implies that the laggers should focus their efforts on developing auditing policies and procedures. Lastly, the followers were less likely to adopt third-party practices than the security leaders (although their adoption levels were a little higher than those of the laggers). Note that regulatory compliance (HITECH, HIPAA, and State) and third party management (breach practices and training) are significantly correlated as Table 2 describes, whereas third-party agreement shows very low correlation. Thus, we can conclude that third party breach management and training play a key role for perceived regulatory compliance (rather than third party agreements), and further those adoption levels differentiate the security leaders from the others.



Note. *Compliance measured on a seven-point scale where 1 -"not at all compliant" and 7 -"compliant with all applicable standards*

Figure 2 The Relationships Between Security Practices and Regulatory Compliance

DISCUSSION

We draw several implications from the findings. First, our results showed that hospitals try to balance practice adoption within the four security domains. For example, the laggers in cluster 3 had widely adopted at least one security practice from each domain (i.e., third-party agreement (0.97), technical IT safeguarding measures (0.93), hiring practices (0.93), and IT audit applications (0.80)). These four practices are ranked first through forth within cluster 3, and further the adoption levels of the first three practices are not significantly different than those of the security leaders in cluster 1. The followers in cluster 2 showed higher levels for practices that were very low for the laggers, while maintaining the laggers' top four practices. Lastly, the security leaders in cluster 1 had highly adopted all security practices in a balanced way. This seems to indicate that hospitals tried first to ensure information security in major security domains by adopting at least one practice, rather than comprehensively adopting practices within any single domain. This may indicate that the current regulatory environment pushes hospitals towards a "cover the bases" approach rather than deep adoption within any particular security domain.

Second, hospitals likely put highest priority on adopting technical solutions (i.e., firewalls, encrypted e-mails, network monitoring, intrusion detection etc.) rather than security management processes. Similarly, in terms of auditing, they more frequently adopted IT applications to support audit functions than developing audit procedures. Despite the hospitals' high adoption of technical solutions, their reported compliance levels varied. This compliance variation seems to be associated with the adoption levels of policies and procedures, suggesting that deploying non-technical solutions with technical solutions is important for improved regulatory compliance.

Third, hospitals with lower compliance preferred one-time practices like hiring practices (e.g., background checking) or third-party agreements to cultural practices like education or developing security procedures. Improving cultural practices would be more difficult, since it requires all employees and organization partners to be involved in developing a mature security culture. As shown in Table 2, the level of regulatory compliance is more closely associated with cultural practices than one-time third-party agreements.

Lastly, security practices have different effects on compliance levels. Our results indicate that the laggers in cluster 3 should focus on auditing solutions, while the followers need to better manage third-party breaches and training.

Regarding the levels of hospitals' compliance and security practices adoption, policy makers should provide guidelines that balance adoption between technical and non-technical solutions and between one-time vs. cultural tasks.

Limitations

Although this study sheds light on the security practices and compliance, it is important to acknowledge the limitations. The survey data was self-reported by IT managers including IT executives, Chief Security Officers (CSO), Health Information Management (HIM) Directors, Compliance Officers and Privacy Officers in each participating organization. Therefore, our results are based on managerial perceptions of security practices and regulatory compliance.

CONCLUSIONS

We examined the adoption of security practices, with the goal of identifying dominant configurations, and their relationship to perceived compliance. Using survey data that provided the status of adopted security practices, we clustered 204 hospitals into three groups. Clusters were based on practice similarities and associated compliance levels. While hospitals across all three clusters widely adopted technical practices, we found significant differences among non-technical practices. Further, we demonstrated that audit practices play a critical role in the improved compliance we observed in the followers, while third-party breach management and training were important to reach the highest levels of compliance found among the leaders in cluster 1.

ACKNOWLEDGMENTS

The authors would like to thank Kroll Fraud Solutions and the Health Information and Management Systems Society (HIMSS) Foundation for sharing survey data.

REFERENCES

1. Beard, L., Schein, R., Morra, D., Wilson, K. and Keelan, J. (2012) The challenges in making electronic health records accessible to patients, *Journal of the American Medical Informatics Association*, 19, 1, 116-120.
2. Collmann, J. and T. Cooper (2007). Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security, *Journal of the American Medical Informatics Association*, 14, 2, 239-243.
3. D'Arcy, J., Hovav, A. and Galletta, D. (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, 20, 1, 79-98.
4. Ferratt, T.W., Agarwal, R., Brown, C.V. and Moore, J.E. (2005) IT human resource management configurations and IT turnover: Theoretical synthesis and empirical analysis, *Information Systems Research*, 16, 3, 237-255.
5. Herath, T. and Rao, H.R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organizations, *European Journal of Information Systems*, 18, 2, 106-125.
6. HHS (2005) the Summary of Nationwide Health Information Network Request for Information Responses, Washington, D.C.
7. SAS Institute. (1990) SAS/STAT user's guide (Release 6.00), N. Cary.
8. ITGI (2005) Board Briefing on IT Governance. ISACA, The IT Governance Institute (ITGI).
9. Johnston, A. C. and Warkentin, M. (2010) Fear Appeals and Information Security Behaviors: An Empirical Study." MIS Quarterly 34, 3, 549-566.
10. Kayworth, T. and Whitten, D. (2010) Effective Information Security Requires a Balance of Social and Technology Factors, *MIS Quarterly Executive*, 9, 3, 163-175.
11. Milligan, G. W. and Cooper, M. C. (1985) An Examination of Procedures for Determining the Number of Clusters in a Data set, *Psychometrika* 50, 2, 159-179.
12. Murphy, S. N., Gainer, V., Mendis, M., Churchill, S. and Kohane, I. (2011) Strategies for maintaining patient privacy in i2b2, *Journal of the American Medical Informatics Association*, 18, 1, 103-108.
13. Pavolotsky, J. (2011) Compliance Best Practices for Information Security: A Perspective, Corporate Compliance Insights.
14. Puhakainen, P. and Siponen, M. (2010) Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, *MIS Quarterly*, 34, 4, 757-778.
15. Ravichandran, T. and Rai, A. (1999) Total quality management in information systems development: Key constructs and relationships, *Journal of Management Information Systems*, 16, 3, 119-155.
16. Siponen, M. and Vance, A. (2010) Neutralization: New Insights into the Problem of Employee Information systems Security Policy Violations, *MIS Quarterly* 34, 3, 487-502.
17. Spears, J.L. and Barki, H. (2010) User Participation in Information Systems Security Risk Management, *MIS Quarterly*, 34, 3, 503-522.
18. Urbaczewski, A. and Jessup, L. M. (2002) Does electronic monitoring of employee Internet usage work?, *Communications of the ACM*, 45, 1, 80-83.