

# Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables

INQUIRY: The Journal of Health Care  
Organization, Provision, and Financing  
Volume 58: 1–12  
© The Author(s) 2021  
Article reuse guidelines:  
sagepub.com/journals-permissions  
DOI: 10.1177/00469580211029599  
journals.sagepub.com/home/inq



Kuang-Ming Kuo, PhD<sup>1</sup> , Paul C. Talley, PhD<sup>2</sup>,  
and Dyi-Yih Michael Lin, PhD<sup>2</sup>

## Abstract

Information security has come to the forefront as an organizational priority since information systems are considered as some of the most important assets for achieving competitive advantages. Despite huge capital expenditures devoted to information security, the occurrence of security breaches is still very much on the rise. More studies are thus required to inform organizations with a better insight on how to adequately promote information security. To address this issue, this study investigates important factors influencing hospital staff's adherence to Information Security Policy (ISP). Deterrence theory is adopted as the theoretical underpinning, in which punishment severity and punishment certainty are recognized as the most significant predictors of ISP adherence. Further, this study attempts to identify the antecedents of punishment severity and punishment certainty by drawing from upper echelon theory and well-acknowledged international standards of IS security practices. A survey approach was used to collect 299 valid responses from a large Taiwanese healthcare system, and hypotheses were tested by applying partial least squares-based structural equation modeling. Our empirical results show that Security Education, Training, and Awareness (SETA) programs, combined with internal auditing effectiveness are significant predictors of punishment severity and punishment certainty, while top management support is not. Further, punishment severity and punishment certainty are significant predictors of hospital staff's ISP adherence intention. Our study highlights the importance of SETA programs and internal auditing for reinforcing hospital staff's perceptions on punishment concerning ISP violation, hospitals can thus propose better internal strategies to improve their staff's ISP compliance intention accordingly.

## Keywords

deterrence theory, electronic medical records, internal auditing effectiveness, staffing compliance levels, security education, training and awareness programs, top management support

### What do we already know about this topic?

Punishment severity and punishment certainty are related to security-compliant behavior.

### How does your research contribute to the field?

This study confirms that Security Education, Training, and Awareness programs (SETA) and internal auditing effectiveness are antecedents of punishment severity and punishment certainty.

### What are your research's implications towards theory, practice, or policy?

In addition to stated punishment for violating information security policy, hospitals can provide appropriate SETA programs and then undertake internal auditing to improve their staff's adherence intention of information security policy.

## Introduction

In recent years, information security has been boosted as an organizational priority<sup>1</sup> since most organizations have recognized that information systems (IS) are important assets for achieving competitive advantages. As such, these assets are subject to intrusion, data theft, and corruption.

Consequently, organizations have adopted various information security protection measures such as administrative, technical, and physical security controls at vast expense to prevent all forms of unauthorized usage. A prior report has estimated worldwide information security spending will exceed US \$151 billion by 2023, with a 5-year annual growth rate about 9.4%.<sup>2</sup> Regardless of



Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (<https://creativecommons.org/licenses/by-nc/4.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

such huge capital expenditures devoted to information security, the occurrence of IS security breaches is still very much on the rise.<sup>3</sup> According to a recent important security report,<sup>4</sup> about 90% of large organizations have some form of security breach. And, the healthcare industry is no exception.<sup>5</sup> Among the various security breaches, employees are still considered to be the biggest threat to organizational security.<sup>6</sup> For example, the notorious security breach of the Veterans' Administration Hospitals incident<sup>7</sup>: About 26.5 million discharged veterans' records containing names, social security numbers, and dates of birth, were taken in an unauthorized manner by employees. Or, the Jackson Health System being fined 2.15 million USD by the Department of Health and Services for several data breaches from 2013 to 2016, including evidence that an employee was found selling patients' data.<sup>8</sup> The number of, and source of, security breaches signifies the importance of how much organizations should regulate the usage behaviors of employees.

Moreover, it is commonly acknowledged that technical countermeasures alone are insufficient to ensure organizational security due to neglect of human behaviors.<sup>9,10</sup> To bolster this deficiency, most organizations have formulated information security policies (ISPs) which articulate the procedures and processes that a staff should comply with in order to secure the confidentiality, integrity, and availability of information and other important assets.<sup>11</sup> Based on a prior information security breach report,<sup>4</sup> 98% of large organizations and 60% of small organizations have some kind of stated ISP in place. In words, most organizations are aware of the important role information security policies plays on a daily basis. In Taiwan, the Government has established the National Center for Cyber Security Technology to ensure a safe cyber security environment.<sup>12</sup> Several governing agencies have also fostered security regulations for differing industries<sup>13,14</sup> aimed at regulating information security practices. However, insider breaches still occurred,<sup>15</sup> indicating the issue of ISP compliance deserves ever more attention.

Information security policies, however, will not work if stated rules are not enforced with some degree of regularity.<sup>16</sup> Prior research therefore adopts deterrence theory to examine the impact of a deterrence approach on employees' information security behaviors.<sup>17,18</sup> Deterrence theory is specifically tailored to model how unlawful usage behavior can be prohibited by the threat of severe and certain of punishment.<sup>19</sup>

More specifically, deterrence theory can be used to explain the determinants of avoiding illicit behavior.<sup>20</sup> For instance, a recent huge levy of fines on large organizations due to information breaches indicate clear cases of expecting deterrence to work.<sup>8</sup> More and more, organizations are therefore spending 50% or more of their funds on information security practices such as risk reduction or changing or fulfilling new compliance requirements to proscribe huge fines.<sup>21</sup> However, the method of how to reinforce the threatening perceptions of punishment remains understudied and thus unclear in deterrence theory. Ideally a model/theory is expected to be helpful in both prediction and explanation,<sup>22</sup> it is therefore essential to further extend deterrence theory by inspecting the effects of potential antecedents on severe and certain punishment. By doing so, organizations can acquire a better insight on information security and thus propose a better strategy to protect the security of important informational assets accordingly.

The main purpose of this study is, based on deterrence theory, 2-fold: (1) to investigate the antecedents of and their effects on punishment severity and punishment certainty, and (2) to examine the effects of punishment severity and punishment certainty on hospital staff's intention to comply with ISP. We investigated intention rather than actual behavior since intention is not an absolute predictor of actual behavior in an information security context.<sup>23,24</sup> We therefore hold that intention should first become well understood and then we can investigate actual information security behavior. The ISP in our study refers to a generic information security policy which is formulated by hospitals based on their differing organizational characteristics but conforming to the regulations of the Ministry of Health and Welfare in Taiwan.<sup>14</sup> Since more and more healthcare facilities have adopted Electronic Medical Records (EMR), how to further safeguard these important information assets deserves more attention and better investigation.

## Theoretical Foundation, Research Model and Hypotheses

### *Deterrence Theory*

Rooted in criminology, deterrence theory aims to diminish illicit behaviors of potential perpetrators via severe, certain, and swift punishment.<sup>20,25</sup> In light of these punishments, rational perpetrators will evaluate the trade-off between the

<sup>1</sup>National United University, Miaoli, Taiwan, R.O.C.

<sup>2</sup>I-Shou University, Kaohsiung City, Taiwan, R.O.C.

Received 17 March 2021; revised 27 May 2021; revised manuscript accepted 14 June 2021

#### **Corresponding Authors:**

Kuang-Ming Kuo, Department of Business Management, National United University, I, Lienda, Miaoli 360001, Taiwan, R.O.C.

Email: kuangmingkuo@gmail.com

Dyi-Yih Michael Lin, Department of Industrial Management, I-Shou University, No. 1, Sec 1, Syuecheng Rd., Dashu District, Kaohsiung City 84001, Taiwan, R.O.C.

Email: dlin@isu.edu.tw

potential gains and proscribed losses before committing illegal behaviors. Three constructs including punishment severity, punishment certainty, and punishment celerity, were developed to conceptualize the main spirit of a deterrence approach.<sup>19</sup>

Punishment severity means the level of severity applied in terms of punishment for the undertaking of illegal behavior, while punishment certainty is considered to be a specific type of punishment certain to be enforced if illicit behavior is to be conducted.<sup>19,20</sup> Finally, punishment celerity, which is less adopted due to methodological considerations,<sup>19,20</sup> refers to the speed of punishment taking place after the occurrence of illegal behavior.<sup>19,20</sup> Deterrence theory has been widely adopted to investigate security-compliant and security-risk related behaviors in differing industries.<sup>26,27</sup> Despite some literature demonstrative of conflicting results, meta-analysis evidence shows that deterrence constructs including punishment severity/certainty/celerity correlate with security-compliant and security-risk behaviors, both positively and negatively, respectively.<sup>28,29</sup>

### *Antecedents of Deterrent Variables*

Knowing severity of and certainty of punishment are correlated with security-compliant or security-risk behaviors is important; it is, however, only the halfway of gaining a deeper knowledge of security issues relevant to data management. What is more important is how to effectively reinforce individual's perceptions concerning punishment severity and punishment certainty. Up to now, there have been only a few studies focused on the antecedents of punishment severity and punishment certainty.<sup>17,18,30-32</sup> These studied antecedents include fear, anger,<sup>31</sup> procedural, and technical countermeasures,<sup>18</sup> self-efficacy,<sup>32</sup> security policy, security education, and training programs, computer monitoring,<sup>17</sup> organizational size, industry type, and top management support.<sup>30</sup> These studies have surely paved the way for further investigating of the important antecedents of deterrent variables based on deterrence theory. As previously stated, some study findings are rather mixed. For example, D'Arcy et al<sup>17</sup> proposed a model for predicting IS misuse intention. One of the proposed hypotheses related to the association of security policies and perceived certainty of sanctions. They found these 2 variables significantly correlative but their correlation was in a negative direction (ie, diametrically opposed). Further, 3 out of 5 studies adopted variables that were pertinent to organizations rather than to individuals. The evidence reviewed here seems to highlight the need for subsequent research on organizationally related variables as antecedents of deterrents based on deterrence theory.

### *Research Model and Hypothesis Formulation*

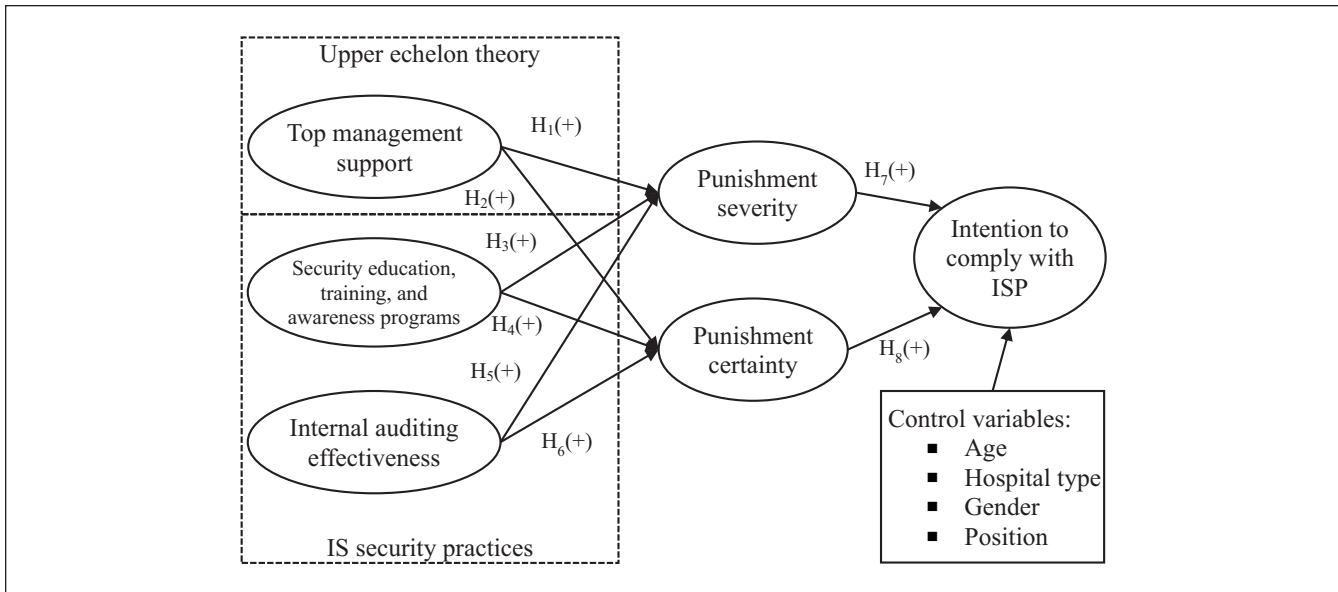
To fulfill our study purposes, we adopted deterrence theory as the primary theoretical basis. As with the above-discussion,

deterrence theory has long-presumed that unlawful behavior can be discouraged via severe and certain punishments.<sup>25,33</sup> As such, punishment severity and punishment certainty should be able to regulate hospital staff to comply with ISP. Our model did not encompass celerity of punishment mainly due to its weak effect on security-compliant intention<sup>28</sup> and also difficulties in measurement.<sup>19</sup>

In our quest to arrive at the antecedents of punishment severity and punishment certainty, we drew from upper echelon theory<sup>34</sup> and well-acknowledged international standards of IS security practices.<sup>35-38</sup> According to upper echelon theory,<sup>34</sup> organizational strategic decisions are made based on top management's values and cognitive base. In other words, top management support influences an organization and organizational behavior in various ways.<sup>34,39</sup> Further, IS security practices<sup>36</sup> clearly articulate that top management shall demonstrate a commitment to information security issues. Hence, we can expect that top management support can reinforce hospital staff's perceptions of punishment severity and punishment certainty. Moreover, Security Education, Training, and Awareness (SETA) programs and internal auditing are both key components for implementing security control.<sup>35-38</sup> The goal of SETA programs is to enable staff to acquire competent IS security skills/knowledge and to be aware of IS policy, while internal auditing is to ensure IS security control conforms to organizational requirements and international standards.<sup>36</sup> Via appropriate SETA programs and better internal auditing effectiveness, hospital staff will be informed of the pertinent sanctions for ISP violation.<sup>37</sup> Further, we hypothesize that hospital staff's compliance intention with ISP can be predicted by punishment severity and punishment certainty according to deterrence theory. Although these factors for ISP compliance have been examined in prior literature, there remains a paucity of evidence considering all the important factors taken simultaneously since they were usually investigated in isolation.

In order to prevent the unexpected influence of some demographic variables on the analysis results, we included age (5 categories), hospital type (3 categories), gender (2 categories), and position (4 categories) as control variables in our proposed model. All control variables were dummy-coded for the purpose of subsequent analysis. The explication of (*see* Figure 1) and the constructs and their relationships in the proposed research model are manifested as follows.

*Effect of top management support on punishment severity, punishment certainty, and hospital staff's adherence to ISP.* In our study, top management support of ISP refers to a commitment to IS security from the upper-level management in hospitals, as observed by employees.<sup>40</sup> Punishment severity refers to hospital staff's perceived degree of punishment related to violating ISP, while punishment certainty refers to hospital staff's perceived certainty of being punished when violating ISP.<sup>41</sup> According to upper echelon theory,<sup>34</sup> top management influences an organization in differing



**Figure 1.** Research model.

ways including changing organizational behavior.<sup>39</sup> Within an informational security context, top management support signals the importance of information security to the organization<sup>42</sup> including relevant sanctions to ensure ISP achieving its intended outcomes.<sup>36</sup> In the literature, top management support is confirmed an imperative factor for various organizational initiatives such as the implementation of IS,<sup>43,44</sup> fraud mitigation,<sup>45</sup> and IS security issues.<sup>40,46,47</sup> This support may take the form of guidance or participation in those activities, and more importantly, top management support can secure adequate resources for relevant initiatives to take place. Prior evidence demonstrates that top management support relates to various IS security compliance<sup>40,46,48</sup> or improving an employee's norms.<sup>42</sup> However, there are limited dividends for the effects of top management support on punishment severity and punishment certainty and also for the indirect effects of top management support on hospital staff's adherence to ISP due to punishment severity and punishment certainty. In our study context, if top management shows a high level of support in IS security initiatives and then foster a positive organizational security culture, hospital staff's norms relevant to information security is expected to be influenced and will be more serious about ISP. In other words, hospital staff may consider the possible severity of and certainty of punishment and result in subsequent ISP compliance measures. We therefore hypothesize that:

H1: Greater top management support will result in hospital staff's greater punishment severity perception about ISP compliance.

H1a: The relationship between top management support and hospital staff's intention to comply with ISP will be

indirect and mediated by individual perceptions of punishment severity.

H2: Greater top management support will result in hospital staff's greater punishment certainty perception about ISP compliance.

H2a: The relationship between top management support and hospital staff's intention to comply with ISP will be indirect and mediated by individual perceptions of punishment certainty.

*Effect of security education, training, and awareness programs on punishment severity, punishment certainty, and hospital staff's adherence to ISP.* SETA programs are generally designed and implemented based on organizational security policy which regulates the information security practices of an organization.<sup>11</sup> Relevant security rules and punishments for violation of security policy are typically announced in such SETA programs aiming to be used as a deterrent in order to prevent employees from violating organizational ISP.<sup>36,37</sup> In our study, SETA programs refer to hospital staff's perceived level of proficiency on common knowledge of information security environment, along with required information security skills provided by hospitals.<sup>49</sup> Prior evidence confirms that a SETA program can improve employees' self-efficacy on security,<sup>50</sup> motivate employees to comply with security policy,<sup>51</sup> and increase employees' perceptions concerning punishment severity and punishment certainty.<sup>17</sup> Therefore, hospital staff who attend these SETA programs are expected to possess a deeper knowledge about punishments of non-compliance to the ISP in addition to regular security policies and procedures. In addition to the potential effects of SETA programs on punishment severity and punishment certainty,



the indirect effects of SETA programs on hospital staff's adherence to ISP, via punishment severity and punishment certainty, can therefore be reasonably expected. Based on the above-discussion, we therefore postulate the following hypotheses:

H3: Hospital staff's awareness of a SETA program is positively related with perceived punishment severity.

H3a: The relationship between SETA programs and hospital staff's intention to comply with ISP will be indirect and mediated by individual perceptions of punishment severity.

H4: Hospital staff's awareness of a SETA program is positively related with perceived punishment certainty.

H4a: The relationship between SETA programs and hospital staff's intention to comply with ISP will be indirect and mediated by individual perceptions of punishment certainty.

*Effect of internal auditing effectiveness on punishment severity, punishment certainty, and hospital staff's adherence to ISP.* Internal auditing traditionally concentrates on monitoring financial compliance and internal control, but it has turned into a wider role for the risk management of organizations.<sup>52</sup> It aims to improve an organization's overall operations and adds value to an organization.<sup>53,54</sup> In recent years, the size and role of internal audits has grown significantly in differing industries.<sup>53,55-57</sup> Ahmad et al<sup>58</sup> found that employees' awareness of security monitoring practices enhances security assurance behavior. In the healthcare industry, Hanskamp-Sebregts et al<sup>59</sup> found that medication safety and information security practiced in the wards improved significantly after implementing internal auditing. In our study, we conceptualize internal auditing as internal auditing effectiveness which refers to the degree to which security audits improve the security environment in hospitals.

In the context of information security, internal auditing monitors employees in terms of relevant information security practices, aiming to emphasize the importance of information security and what is expected of the staff.<sup>42</sup> Evidence shows that internal auditing improves information security practices. For example, Steinbart et al<sup>53</sup> found that if internal auditing and information security functions are in a good relationship, information security effectiveness may be improved upon. Cuganesan et al<sup>42</sup> demonstrated that information security monitoring positively improves employee's perceived norms about information security. Hence, hospital staff, if they perceive the effectiveness of internal auditing, will consider the potential severity of and certainty of punishment before they violate ISP, and thus guarantee adherence to ISP. This also means internal auditing effectiveness may exert indirect effects on hospital staff's IPS compliance through punishment severity and punishment certainty. This is in addition to the direct effects of internal auditing effectiveness on punishment severity

and punishment certainty. Based on previous evidence and discussions, we hypothesize that:

H5: Hospital staff's perceived internal auditing effectiveness is positively related with their perceived punishment severity

H5a: The relationship between internal auditing effectiveness and hospital staff's intention to comply with ISP will be indirect and mediated by individual perceptions of punishment severity.

H6: Hospital staff's perceived internal auditing effectiveness is positively related with their perceived punishment certainty.

H6a: The relationship between internal auditing effectiveness and hospital staff's intention to comply with ISP will be indirect and mediated by individual perceptions of punishment certainty.

*Effect of punishment severity on hospital staff's intention to comply with ISP.* In this study, intention to comply with ISP refers to the subjective probability of hospital staff practicing compliance with ISP in the future.<sup>60</sup> According to deterrence theory, as the degree of punishment increases, individuals will be less likely to conduct unlawful behaviors.<sup>61</sup> In other words, punishment can have a deterrent effect on offenders.<sup>62</sup> Transferring this rationale to our study, hospital staff will be more likely to comply with ISP when they perceive the severity of punishment whenever violating ISP. Prior evidence based on deterrence theory has proven that punishment severity can compel employees to adhere to ISP<sup>18,48</sup> or prevent employees from violating ISP.<sup>17</sup> According to the above discussions, we propose the additional hypothesis:

H7: Hospital staff's perceptions of punishment severity will be positively related to their intention to comply with ISP.

*Effect of punishment certainty on hospital staff's intention to comply with ISP.* Organizational rules, in fact, will not come into effect if they are not enforced.<sup>16</sup> In other words, proper compelling policies are required for useful security policy implementations.<sup>49</sup> Organizations should therefore make potential perpetrators aware of those enforcement rules in advance.<sup>61</sup> In this vein, if hospital staff are aware of the probability they will be punished when they are caught violating ISP, they will be more likely than not abide by the stated ISP. In information security context, prior studies found that punishment certainty is related to employee's information security behavioral intentions.<sup>18,41</sup> We therefore hypothesize the following hypothesis:

H8: Hospital staff's perceptions of punishment certainty will be positively related to their intention to comply with ISP.

## Methods

### Measures

We undertook a paper-based survey to gather data. The questionnaire used in our study included 2 parts: (1) respondents' demographic information; and, (2) respondents' perceptions regarding top management support, SETA programs, internal auditing effectiveness, punishment severity, punishment certainty, and the stated intention to comply with ISP.

Previously validated survey scales were used and adapted to our study context. Top management support was measured with 3 items adapted from Humaidi and Balakrishnan<sup>40</sup> and Viswesvaran et al.<sup>63</sup> SETA programs was measured by 3 items modified from D'Arcy et al.<sup>17</sup> Internal auditing effectiveness included 3 items adapted from Alzeban and Gwilliam.<sup>52</sup> Punishment severity and punishment certainty utilized 3 and 3 items, and were adjusted from Herath and Rao<sup>62</sup> and Siponen and Vance,<sup>64</sup> respectively. Finally, one's stated intention to comply with ISP used 3 items adapted from Chen et al.<sup>60</sup> All items were rated according to a 7-point Likert scale. A pilot test was conducted via a sampling of 10 hospital staff, and slight modifications of wording and phraseology were made as a result. The full questionnaire is given in the Appendix.

### Sampling

A survey methodology using paper-and-pencil questionnaires was employed to test the proposed hypotheses. Participants in our study were employees, including healthcare professionals and administrative staff, of a large Taiwanese healthcare system which comprises a medical center, a regional hospital, and a district hospital. The healthcare system is equipped with fully functional EMR and there are 5976 employees existing as potential threats that may jeopardize information security.

Given the considerable workload of hospital employees, a census of all qualified staff is unfeasible, we therefore utilized convenience sampling to assemble required data. Further, to achieve the acceptable 80% statistical power for detecting  $R^2$  values of at least 0.1 (with a 5% significance level), at least 103 samples are required for our model.<sup>65</sup> Considering the feasibility of data collection, and to achieve a higher statistical power, we therefore distributed 300 questionnaires to the medical center, regional hospital, and district hospital of the subject healthcare system roughly based on the stratification of qualified respondents from these hospitals. We designated a coordinator, a staff member of the healthcare system, responsible for distributing and collecting questionnaires for the departments who is willing to participate in our study, and 300 responses were returned. One questionnaire was removed due to the incomplete responses present. As a result, 299 suitable responses remained for later analysis. Those hospital staff who participated in the survey did so voluntarily and anonymously. We acquired ethical

approval from the subject hospital before to the administration of the survey.

## Results

### Descriptive Statistics

Of the 299 valid responses, most respondents were collected from the medical center (47.49%) and the regional hospital (40.80%). The majority of the respondents (74.5%) were aged between 30 and 49 years old. Female respondents (70.57%) were more prevalent than males. Most respondents were university-educated (71.57%) and were employed as nurses (33.78%). In addition, over half of those surveyed reported 11 to 30 years of work experience in the healthcare industry (56.52%). Details of the respondents are shown in Table 1.

### Measurement Model

The PLS technique of structural equation modeling, which encompasses the evaluation of measurement model and structural model,<sup>65</sup> was adopted for purposes of analysis. In the assessment of measurement model, we assessed the reliability and validity of measurement items and constructs adopted in our study. Prior literature<sup>65</sup> suggested that item loadings of 0.7 are sufficient for the indicators (*see* Table 2). Further, both composite reliability and Cronbach's  $\alpha$  for each of the constructs were higher than 0.7 threshold, indicating adequate reliability.<sup>65</sup> Fornell and Larcker<sup>66</sup> signified that average variance extracted (AVE) should be above 0.5 to demonstrate sufficient construct convergent validity, which is just the case in our study. Finally, discriminant validity was confirmed based on Heterotrait-Monotrait ratio of correlations (HTMT) since all the correlations between constructs were lower than the most conservative 0.85 criteria,<sup>67</sup> as shown in Table 2. Since some correlations among the constructs were higher than 0.7, we further used tolerance to assess a collinearity problem. The results showed that the tolerance value of each item was above 0.1, demonstrating that collinearity should not be an issue in this study.<sup>68</sup> Further, we assessed common method bias via full collinearity test.<sup>69</sup> Results show that the highest full collinearity variance inflation factor is 2.93 for punishment certainty, as such lower than the suggested threshold of 3.3,<sup>70</sup> indicating common method bias should not be a major concern in this study.

### Structural Model

In PLS, the structural model is used to assess the significance of hypothesized relationships, and the strength of those relationships.<sup>68</sup> As shown in Figure 2, 6 out of the 8 proposed hypotheses were supported.

For the first purpose of investigating the antecedents of and their effects on punishment severity and punishment

**Table 1.** Respondent Characteristics.

Characteristic	Attribute	Frequency	Percentage
Hospital	Medical center	142	47.49
	Regional hospital	122	40.80
	District hospital	35	11.71
Age	20-29	38	12.71
	30-39	109	36.45
	40-49	114	38.13
	50-59	32	10.70
	≥60	6	2.01
Gender	Male	88	29.43
	Female	211	70.57
Education	High school	6	2.01
	College	16	5.35
	University	214	71.57
	Graduate school	63	21.07
Profession	Physician	57	19.06
	Nurse	101	33.78
	Other healthcare professionals (radiological technologist, pharmacist, . . .)	81	27.09
	Administrative staff	60	20.07
Working experience (years)	1-10	123	41.14
	11-20	111	37.12
	21-30	58	19.40
	≥31	7	2.34

**Table 2.** Reliability and Validity.

Construct	# of items	M	SD	Loadings	CR	CA	AVE	Heterotrait-monotrait ratio of correlations						
								TMS	SETA	IAE	PS	PC	ICISP	
Top management support (TMS)	3	5.44	0.92	0.87-0.93	0.93	.89	0.81							
Security education, training, and awareness program (SETA)	3	4.90	1.08	0.95-0.97	0.98	.96	0.93	.54						
Internal auditing effectiveness (IAE)	3	5.51	0.92	0.95-0.97	0.97	.95	0.91	.61	.45					
Punishment severity (PS)	3	5.80	0.90	0.88-0.95	0.94	.91	0.84	.51	.69	.53				
Punishment certainty (PC)	3	4.80	1.13	0.88-0.96	0.95	.92	0.87	.52	.82	.47	.81			
Intention to comply with ISP (ICISP)	3	5.63	0.95	0.98-0.99	0.99	.95	0.97	.47	.74	.35	.73	.76		

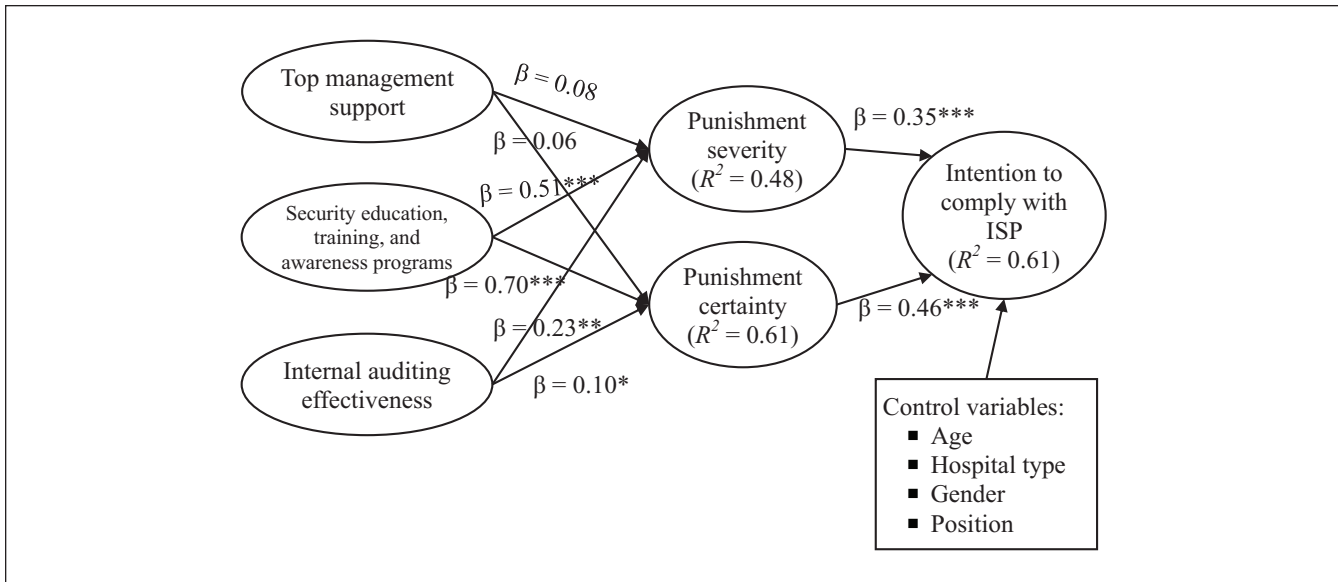
Note. ISP=information security policy; M=average score; SD=standard deviation; CR=composite reliability; CA=Cronbach's  $\alpha$ ; AVE=average variance extracted.

certainty, 4 out of 6 related hypotheses were supported. First of all, there was no evidence that top management support significantly associated with punishment severity ( $\beta=0.08, t=0.99$ ) and punishment certainty ( $\beta=0.06, t=1.29$ ), thus un-supportive of H1 and H2. SETA programs were positively and significantly associated with punishment severity ( $\beta=0.51, t=7.88$ ) and punishment certainty ( $\beta=0.70, t=16.75$ ), respectively. H3 and H4 were both supported. Internal auditing effectiveness was found to significantly relate to punishment severity ( $\beta=0.23, t=2.61$  and punishment certainty ( $\beta=0.10, t=2.34$ ) in a positive direction, respectively. H5 and H6 were supported.

Concerning the second purpose of examining the effects of punishment severity and punishment certainty on hospital

staff's intention to comply with ISP, punishment severity ( $\beta=0.35, t=4.83$ ) and punishment certainty ( $\beta=0.46, t=6.61$ ) positively and significantly associated with intention to comply with ISP, respectively. Hypothesis H7 and H8 were supported.

With regard to variance explained in our model, top management support, SETA programs, and internal auditing effectiveness jointly explained about 48% and 61% of the variance of punishment severity and punishment certainty, respectively. Overall, stated intention to comply with ISP can be accounted for about 61% variance by our proposed model. Further, the hypothesis-testing results were unchanged even after controlling for potential confounding variables (ie, age, hospital type, gender, and position).



**Figure 2.** Structural model results.

Note. ISP = information security policy.

\* $P < .05$ . \*\* $P < .01$ . \*\*\* $P < .001$ .

### *Indirect Effects of Top Management Support, SETA Programs, and Internal Auditing Effectiveness on Hospital Staff's Adherence to Information Security Policy*

We not only investigated the antecedents of punishment severity and punishment certainty, we also investigated the total effects of and significance of the antecedents on hospital staff's adherence to ISP. By doing so, we can further understand whether the antecedents can exert effects, via punishment severity and punishment certainty, indirectly on hospital staff's adherence to ISP, further supporting the importance of antecedents. We followed suggested procedures<sup>71</sup> for assessing the mediating effects of perceived severity and perceived certainty. As depicted in Table 3, perceived severity was confirmed to significantly mediate the relationships between SETA programs/internal auditing effectiveness and intention to comply with ISP, but not the association between top management support and one's intention to comply with ISP. Therefore, H2a and H3a were supported while H1a was not confirmed. Further, punishment certainty was proved to significantly mediate between only the link between SETA programs and intention to comply with ISP but not the relations between top management support/internal auditing effectiveness and intention to comply with ISP. Hence, H5a was confirmed, while H4a and H6a were unsupported. As shown in Table 3, all confirmed mediation were partial mediation.<sup>71</sup>

## **Discussion**

The aims of this study are: (1) to investigate the antecedents of and their effects on punishment severity and punishment

certainty, and (2) to examine the effects of punishment severity and punishment certainty on hospital staff's intention to comply with ISP. According to analysis results, SETA programs and internal auditing effectiveness, but not top management support, significantly related to punishment severity and punishment certainty, respectively. Punishment severity and punishment certainty significantly associated with hospital staff's adherence to ISP. Further, SETA programs and internal auditing effectiveness significantly influence hospital staff's ISP adherence intention indirectly via punishment severity and punishment certainty. Several important implications can be acquired from our findings.

Despite prior evidence supportive of the notion that top management support is an important component in the organizational management of information security issues.<sup>1,48,72</sup> Surprisingly, top management support (H1 and H2), in this study, was not found to be significantly associated with punishment severity and punishment certainty; that is, hospital staff's views on punishment severity and punishment certainty were not impacted or seemingly influenced by hospital managers. This finding contrasts with earlier findings<sup>42</sup> which have suggested that senior management support positively associated with employee's norms regarding information security compliance. There is however a possible explanation for this occurrence. It is argued that the integrity of information security is different from other information technologies since users are not involved in direct interaction with a specific IS.<sup>73</sup> Unlike the implementation of an information technology, or of an IS, hospital staff is unable to map information security with any specificity of information hardware or software, directly. The support of hospital administration on information security may therefore be



**Table 3.** Results of Mediation Analysis.

Mediator	Path	Direct effect			Indirect effect			Mediation effect of PS/PC
		$\beta$	SE	95% CI	$\beta$	SE	95% CI	
Perceived severity (PS)	TMS→PS	.08	0.08	[-0.05, 0.22]				
	SETA→PS	.51	0.04	[0.37, 0.61]				
	IAE→PS	.23	0.04	[0.07, 0.38]				
	TMS→PS→COM				.03	0.02	[-0.02, 0.08]	No mediation
	SETA→PS→COM				.18	0.03	[0.10, 0.27]	Partial mediation
	IAE→PS→COM				.08	0.02	[0.03, 0.15]	Partial mediation
Perceived certainty (PC)	PS→COM	.35	0.08	[0.22, 0.50]				
	TMS→PC	.06	0.05	[-0.01, 0.17]				
	SETA→PC	.70	0.06	[0.61, 0.76]				
	IAE→PC	.10	0.04	[0.03, 0.18]				
	TMS→PC→COM				.03	0.02	[-0.03, 0.09]	No mediation
	SETA→PC→COM				.32	0.04	[0.22, 0.44]	Partial mediation
	IAE→PC→COM				.05	0.02	[-0.01, 0.11]	No mediation
	PC→COM	.46	0.04	[0.31, 0.59]				

Note. TMS=top management support; SETA=security education, training, and awareness programs; IAE=internal auditing effectiveness; COM=intention to comply with ISP.  $\beta$ =path coefficient; SE=standard deviation; CI=confidence interval.

obscure to hospital staff, which results in the insignificant results as the influence of top management support on hospital staff's perceptions about punishment severity and punishment certainty.

Prior evidence reports that SETA programs play an important role in motivating employees to comply with ISP,<sup>51</sup> little evidence however investigates the effect of SETA programs on punishment severity and punishment certainty. Our study showed that SETA programs have a positive effect on hospital staff's perceived punishment severity and punishment certainty (H3 and H4), specifically in the healthcare industry. With appropriate and adequate SETA programs, hospital staff not only will have a general awareness of security knowledge and skills but also will be familiar with relevant punishment whenever violating ISP, just like the findings in our study indicated. Our results corroborate the findings of D'Arcy et al,<sup>17</sup> which was conducted in multiple industries but non-inclusive of the healthcare industry. Further, our finding also reflects the results of Yoo et al<sup>50</sup> who found that SETA programs indirectly influence ISP compliance intention via self-efficacy. The finding of our research draws attention to the importance of allocating more resources to the SETA programs used by hospitals, and ongoing SETA programs should not be neglected or discontinued.

Internal auditing aims to focus resources on meeting potential deficiencies and errors in order to help organizations to avoid their recurrence.<sup>57</sup> Our study found that internal auditing effectiveness positively and significantly is associated with punishment severity and punishment certainty (H5 and H6). In other words, the better the effectiveness of internal auditing, the hospital staff will perceive a higher degree of punishment severity and punishment certainty, empirically supporting the assertion of auditing

activities that can help managerial control take effect.<sup>55,74</sup> Prior evidence showed that computer monitoring practices, 1 type of internal auditing activities,<sup>57</sup> enhance employee's security assurance behavior.<sup>58</sup> Cuganesan et al<sup>42</sup> found that monitoring and evaluation of information security practices significantly associated with employee's norms about information security compliance, which accords with our finding. Thus, our finding may imply that internal auditing emphasis expected information security behaviors of staff and may help reinforce organizational norms including the punishment of non-adherence to ISP. Hospital staff could also have learning opportunities regarding ISP compliance since internal auditing affords feedback reports. Hospitals can thus increase staff's perceived severity and certainty of punishment for ISP violation via improving internal auditing effectiveness despite auditees often developing resistance to such a practice.<sup>57</sup>

Aligned with the notion of deterrence theory,<sup>19</sup> we found that punishment severity and punishment certainty associate with hospital staff's stated intentions to adhere to ISP (H7 and H8). In other words, hospital staff will demonstrate their intention to comply with ISP if they perceive a higher degree of punishment severity and punishment certainty. These findings are consistent with the literature,<sup>41</sup> and they may suggest that hospitals should have stated disciplinary regulations and processes which include severe and certain sanctions when employees violate existing ISP.

Regarding mediation effects, we found that punishment severity and punishment certainty have no mediation effect between top management support and any intention to comply with ISP. It may be that the effects of top management support on punishment severity and punishment certainty were too miniscule to have a significant indirect effect on

hospital staff's stated intention to comply with ISP. We however found that punishment severity and punishment certainty significantly mediate between SETA programs and hospital staff's stated intention to comply with ISP; that is, SETA programs can influence hospital staff's intention to comply with ISP indirectly. These results may further reflect the importance of SETA programs to positively affect EMR security. Finally, we only found that punishment severity has a mediation effect between internal auditing effectiveness and hospital staff's stated intention to comply with ISP, but not with punishment certainty. A plausible explanation for this may be that currently no employee of the healthcare system has a record of punishment for violating ISP which would result in such a specific finding. It may further be proven that the mean scores (4.8) of punishment certainty is the lowest among all constructs in this study.

As opposed to information provided through questionnaires, document analysis could have also provided evidence of top management support, training, and some intervention for deterrence. Future research could employ document analysis for further support of the results. Finally, our study only collected data from 1 healthcare system in Taiwan. In other words, the generalizability of our findings is limited. Future research can focus on this issue and collect a wider range of regional or national hospitals to advance the topic.

## Conclusion

The primary purposes of this study are to: (1) investigate the antecedents of and effects of punishment severity and punishment certainty, and (2) examine the effects of punishment severity and punishment certainty on hospital staff's stated intention to comply with ISP. To achieve these goals, we adopted deterrence theory as the major theoretical underpinning combining upper echelon theory and IS security practices for this study. A total of 299 valid responses were collected and analyzed. Results demonstrated that 6 out of 8 of the proposed hypotheses were supported; however, we were not able to confirm the associations between top management support and punishment severity/certainty. Further, we conducted a mediation analysis of punishment severity/certainty. Results showed that punishment severity partially mediates between SETA programs/internal auditing effectiveness and hospital staff's stated intention to comply with ISP, while punishment certainty mediates only between SETA programs and hospital staff's intention to comply with ISP. Based on our findings, hospitals, in addition to fostering regulations outlining stated punishment of non-adherence to ISP, can continue to provide staff with appropriate SETA programs that will acquaint staff with regular security policies and regulations. Most importantly, SETA programs should clearly communicate that staff account for their own security actions since a formal disciplinary process is in place in ISP. Further, hospitals should undertake required internal auditing, both periodically and irregularly, on staff's

security activities, exceptions, faults, and information security events to ensure staff's real adherence to ISP. By focusing on SETA programs and internal auditing, hospitals can therefore reinforce staff's perceptions on the severity of and certainty of punishment to better regulate staff's ISP adherence intention in a positive manner.

## Acknowledgments

This work was supported by the Medical Center Research Project (Grant no. ISU-109-MCRP-04), I-Shou University, Taiwan, R.O.C.

## Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.


## Ethical Approval

The Institutional Review Board of Chi-Mei Medical Center approved the study and waived the mandate for written informed consent (#10906-009).

## Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Medical Center Research Project (Grant no. ISU-109-MCRP-04), I-Shou University, Taiwan, R.O.C.

## ORCID iD

Kuang-Ming Kuo  <https://orcid.org/0000-0002-8552-3016>

## Supplemental Material

Supplemental material for this article is available online.

## References

1. Herath T, Herath H, Bremser WG. Balanced scorecard implementation of security strategies: a framework for IT security performance management. *Inf Syst Manag*. 2010;27(1):72-81.
2. Massey K. Worldwide security forecast, 2019–2023: market opportunity by industry—2H18. 2019. Accessed February 24, 2021. <https://www.idc.com>
3. Symantec. Internet security threat. Accessed April 19, 2019. <https://resource.elq.symantec.com>
4. Price-Waterhouse Coopers. Managing cyber risks in an interconnected world – key findings from the global state of information security survey 2015. 2015. Accessed April 24, 2021. <http://www.pwc.com/gsis2015>
5. U.S. Department of Health and Human Services. Breaches affecting 500 or more individuals. 2021. Accessed February 24, 2021. [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
6. Price-Waterhouse Coopers. Turnaround and transformation in cybersecurity: key findings from the global state of information security. U.S.A. 2016. Accessed April 24, 2021. <http://www.pwc.com/gsis>
7. Stout D. Personal data of 26.5 million veterans stolen. *The New York Times*. Accessed April 24, 2021. <https://www.nytimes.com/2006/05/22/washington/22cnd-identity.html>

8. Swinhoe D. The biggest data breach fines, penalties, and settlements so far. 2021. Accessed April 18, 2021. <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>
9. Vroom C, von Solms R. Towards information security behavioural compliance. *Comput Secur.* 2004;23(3):191-198.
10. Chen H, Chau PYK, Li W. The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Inf Technol People.* 2019; 32(4):973-992.
11. Chen L, Zhen J, Dong K, Xie Z. Effects of sanction on the mentality of information security policy compliance. *Rev Argent Clin Psicol.* 2020;29(1):39-49.
12. National Center for Cyber Security Technology. About NCCST. 2016. Accessed April 18, 2021. <https://www.nccst.nat.gov.tw/About?lang=en>
13. Financial Supervisory Commission. Regulations governing the standards for information system and security management of electronic payment institution. 2017. Accessed April 20, 2021. <https://law.moj.gov.tw>
14. Ministry of Health and Welfare. Regulations governing the utilization and management of electronic medical records among medical facilities. 2009. Accessed April 20, 2021. <http://law.moj.gov.tw>
15. Yu M, Yeh J. Military hackers not charged, were testing website's safety. 2021. Accessed April 20, 2021. <https://focustaiwan.tw/politics/202102070005>
16. Peace AG, Galletta AG, Thong JYL. Software piracy in the workplace: a model and empirical test. *J Manag Inf Syst.* 2003;20(1):153-177.
17. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf Syst Res.* 2009;20(1):79-98.
18. Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. *Inf Manag.* 2012;49(2):99-110.
19. D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur J Inf Syst.* 2011;20(6):643-658.
20. Onwudiwe I, Odo J, Onyeozili E. Deterrence theory. In: Bosworth M, ed. *Encyclopedia of Prisons & Correctional Facilities.* Sage Publications, Inc; 2005:234-238.
21. Earnest & Young. EY global information security survey 2020. 2020. Accessed April 20, 2021. <https://assets.ey.com>
22. Davis FD, Bagozzi RP, Warshaw PR. User acceptance of computer technology: a comparison of two theoretical models. *Manage Sci.* 1989;35(8):982-1003.
23. Merritt C, Dhillon G. What interrupts intention to comply with IS-security policy? Paper presented at: 2016 American Conference on Information Systems; August 11-14, 2016; San Diego, CA.
24. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. *Comput Secur.* 2015;53:65-78.
25. Gibbs JP. Crime, punishment, and deterrence. *Southwest Soc Sci Q.* 1968;48(2):515-530.
26. D'Arcy J, Devaraj S. Employee misuse of information technology resources: testing a contemporary deterrence model. *Decis Sci.* 2012;43(6):1091-1124.
27. Foth M. Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *Eur J Inf Syst.* 2016;25(2):91-109.
28. Kuo KM, Talley PC, Huang CH. A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. *Comput Secur.* 2020;96:101928.
29. Trang S, Brendel B. A meta-analysis of deterrence theory in information security policy compliance research. *Inf Syst Front.* 2019;21:1265-1284.
30. Kankanhalli A, Teo HH, Tan BCY, Wei K-K. An integrative study of information systems security effectiveness. *Int J Inf Manage.* 2003;23(2):139-154.
31. Xue Y, Liang H, Wu L. Punishment, justice, and compliance in mandatory IT settings. *Inf Syst Res.* 2011;22(2):400-414.
32. Zhang J, Reithel BJ, Li H. Impact of perceived technical protection on security behaviors. *Inf Manag Comput Secur.* 2009;17(4):330-340.
33. Tittle CR. Crime rates and legal sanctions. *Soc Probl.* 1969; 16(4):409-423.
34. Hambrick DC, Mason PA. Upper echelons: the organization as a reflection of its top managers. *Acad Manage Rev.* 1984;9(2):193-206.
35. Chopra A, Chaudhary M. *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines.* Apress; 2020.
36. ISO. *ISO/IEC 27001:2013 Information Technology-Security Techniques-Information Security Management Systems-Requirements.* ISO/IEC; 2013.
37. ISO. *ISO/IEC 27002:2013 Information Technology-Security Techniques-Code of Practice for Information Security Controls.* ISO/IEC; 2013.
38. ISO. *ISO/IEC 27701:2019 Security Techniques-Extention to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management-Requirements and Guidelines.* ISO/IEC; 2019.
39. Colwell SR, Joshi AW. Corporate ecological responsiveness: antecedent effects of institutional pressure and top management commitment and their impact on organizational performance. *Bus Strategy Environ.* 2013;22(2):73-91.
40. Humaidi N, Balakrishnan V. Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Inf Manage J.* 2017;47(1):17-27.
41. Kuo KM, Talley PC, Hung MC, Chen YL. A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *J Med Syst.* 2017;41(12):198.
42. Cuganesan S, Steele C, Hart A. How senior management and workplace norms influence information security attitudes and self-efficacy. *Behav Inf Technol.* 2018;37(1):50-65.
43. Sharma R, Yetton P. Top management support and IS implementation: further support for the moderating role of task interdependence. *Eur J Inf Syst.* 2011;20(6):703-712.
44. Hwang MI. Top management support and information systems implementation success: a meta-analytical replication. *Int J Inf Technol Manag.* 2019;18(4):347-361.
45. Alazzabi WYE, Mustafa H, Karage AI. Risk management, top management support, internal audit activities and fraud mitigation. *J Financ Crime.* Published online January 24, 2020. doi:10.1108/jfc-11-2019-0147
46. Brady JW. Securing health care: assessing factors that affect HIPAA security compliance in academic medical centers.

- Paper presented at: 2011 44th Hawaii International Conference on System Sciences; January 4-7, 2011; Kauai, HI.
47. Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: a literature review. *Int J Inf Manage.* 2016;36(2):215-225.
  48. Ifinedo P. Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines? *Inf Syst Manage.* 2016;33(1):30-41.
  49. Herath T, Yim MS, D'Arcy J, Nam K, Rao HR. Examining employee security violations: moral disengagement and its environmental influences. *Inf Technol People.* 2018;31(6):1135-1162.
  50. Yoo CW, Sanders GL, Cerveny RP. Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decis Support Syst.* 2018;108:107-118.
  51. Kim HL, Choi HS, Han J. Leader power and employees' information security policy compliance. *Secur J.* 2019;32:391-409.
  52. Alzeban A, Gwilliam D. Factors affecting the internal audit effectiveness: a survey of the Saudi public sector. *J Int Account Audit Tax.* 2014;23(2):74-86.
  53. Steinbart PJ, Raschke RL, Gal G, Dilla WN. The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Account Organ Soc.* 2018;71:15-29.
  54. The Institute of Internal Auditing. Definition of internal auditing. 2020. Accessed December 20, 2020. <https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx>
  55. Eden D, Moriah L. Impact of internal auditing on branch bank performance: a field experiment. *Organ Behav Hum Decis Process.* 1996;68(3):262-271.
  56. Hanskamp-Sebregts M, Zegers M, Boeijen W, Westert GP, van Gurp PJ, Wollersheim H. Effects of auditing patient safety in hospital care: design of a mixed-method evaluation. *BMC Health Serv Res.* 2013;13(1):226.
  57. Ma'ayan Y, Carmeli A. Internal audits as a source of ethical behavior, efficiency, and effectiveness in work units. *J Bus Ethics.* 2016;137(2):347-363.
  58. Ahmad Z, Ong TS, Liew TH, Norhashim M. Security monitoring and information security assurance behaviour among employees. *Inf Comput Secur.* 2019;27(2):165-188.
  59. Hanskamp-Sebregts M, Zegers M, Westert GP, et al. Effects of patient safety auditing in hospital care: results of a mixed-method evaluation (part 1). *Int J Qual Health Care.* 2019;31(7):8-15.
  60. Chen X, Wu D, Chen L, Teng JKL. Sanction severity and employees' information security policy compliance: investigating mediating, moderating, and control variables. *Inf Manag.* 2018;55(8):1049-1060.
  61. Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decis Support Syst.* 2009;47(2):154-165.
  62. Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur J Inf Syst.* 2009;18(2):106-125.
  63. Viswesvaran C, Deshpande SP, Joseph J. Job satisfaction as a function of top management support for ethical behavior: a study of Indian managers. *J Bus Ethics.* 1998;17(4):365-371.
  64. Siponen M, Vance A. Neutralization: new insights into the problem of employee systems security policy violations. *MIS Q.* 2010;34(3):487-502.
  65. Hair JF, Hult GTM, Ringle CM, Sarstedt M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-PM)*. 2nd ed. Sage; 2017.
  66. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *J Mark Res.* 1981;18(1):39-50.
  67. Henseler J, Ringle C, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J Acad Mark Sci.* 2015;43(1):115-135.
  68. Hair JF, Black WC, Babin BJ, Anderson RE. *Multivariate Data Analysis – A Global Perspective*. 7th ed. Prentice-Hall; 2010.
  69. Kock N, Lynn G. Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations. *J Assoc Inf Syst.* 2012;13(7):546-580.
  70. Kock N. Common method bias in PLS-SEM: a full collinearity assessment approach. *Int J ECollab.* 2015;11:1-10.
  71. Tofighi D, MacKinnon DP. RMediation: an R package for mediation analysis confidence intervals. *Behav Res Methods.* 2011;43(3):692-700.
  72. D'Arcy J, Greene G. Security culture and the employment relationship as drivers of employees' security compliance. *Inf Manag Comput Secur.* 2014;22(5):474-489.
  73. Lowry PB, Dinev T, Willison R. Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *Eur J Inf Syst.* 2017;26(6):546-563.
  74. Chang YT, Chen H, Cheng RK, Chi W. The impact of internal audit attributes on the effectiveness of internal control over operations and compliance. *J Contemp Account Econom.* 2019;15(1):1-19.