Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Information security policies' compliance: a perspective for higher education institutions

Sadaf Hina & P. Dhanapal Durai Dominic

To cite this article: Sadaf Hina & P. Dhanapal Durai Dominic (2018): Information security policies' compliance: a perspective for higher education institutions, Journal of Computer Information Systems, DOI: 10.1080/08874417.2018.1432996

To link to this article: https://doi.org/10.1080/08874417.2018.1432996

Published online: 30 Mar 2018.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2018.1432996

Information security policies' compliance: a perspective for higher education institutions

Sadaf Hina and P. Dhanapal Durai Dominic

Department of Computers and Information Science, Universiti Teknologi PETRONAS, Tronoh, Malaysia

ABSTRACT

This paper provides a systematic literature review in the information security policies' compliance (ISPC) field, with respect to information security culture, information security awareness, and information security management exploring in various settings the research designs, methodologies, and frameworks that have evolved over the last decade. Studies conducted from 2006 to 2016 reporting results from data collected through diverse means have been explored; however, only a few studies have focused primarily on a sensitive infrastructure under risk, as is the case with higher education institutions (HEIs). This study reports that ISPC in HEIs remains scarce, as is the realization of security threats and dissemination of information security policies to end users (employees). This research makes a novel contribution to the body of knowledge as a unique study that has reviewed the influence of institutional governance in HEIs on protection motivation leading towards ISPC.

KEYWORDS

Information security policies' compliance; information security culture; information security management; information security awareness; computer and information systems security

Introduction

Computers and information systems (IS) are key to success in any organization. Ensuring the security of these systems is a vital task that maintains the basic aspects of the information security phenomenon, namely, confidentiality, availability, and integrity. The execution and success of organizational processes rely heavily upon the effective implementation of information technology (IT) resources and the wide-ranging means of ensuring their security. IS security remains the top priority of IT security personnel and top management in business organizations.[1,2] The primary focus of information protection is to maintain the authenticity of information for various business goals. However, a successful attack can damage tangible and intangible resources and result in serious financial, reputational, and asset losses.[3] With advancements in the integration of technology, information security breaches are also occurring at a rapid pace. People with malicious intentions use state-of-the-art gadgets and continue to develop new ways to hack personal and sensitive information. It is therefore necessary to understand the potential of these risks and to take prompt actions to minimize and/or mitigate the hazards associated with malicious breaches through appropriate plans and procedures.[2]

To protect information assets, organizations need to communicate technical and behavioral solutions to their employees.[4] This notably applies to organizations at high risk that do not realize the magnitude of their information sensitivity, such as higher education institutions (HEIs), that are pursuing business goals like any other business organization around the globe. These institutions comprise numerous departments that function to achieve certain goals in the institution's interests. Examples include finance, faculty departments, IT security management, research grants management, visa processing, and infrastructure management, as well as many other departments that operate under the HEI umbrella. These HEIs experience the same threats and vulnerability as other business organizations.[5,6] Lack of policy guidelines, lack of awareness of information security threats, and irregular monitoring of misuse behavior often lead to threatening situations. Da Veiga[7] explained that the vision and strategies developed by the organization's higher management can create an information security culture (ISC). In that study, conducted over an 8-year period, the author suggested that employees who read and understand the information security policies (ISPs) of their organization show a more positive attitude to developing an ISC. In a study by Ismail et al.[5], four HEIs investigated in Malaysia had versions of IT policies comprising various security standards, such as Malaysian Public-Sector Management of Information and Communications Technology Security (MyMIS); International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (ISO/IEC 27001); and Control Objectives for Information and Related Technologies (COBIT). However, none of these HEIs had developed any kind of information security framework to deal with security breaches. In that study's reported data, the technical personnel who participated, such as programmers, system analysts, project managers, IT executives, and IT managers, declared that the faculties and students were the least informed of the awareness programs.[5] This situation has alarmed HEIs that have neglected the end users of their institutional networks and IS. With HEIs' decentralized networks and distributed computing resources, the transfer of information is potentially vulnerable.[6] Hence, HEIs need a holistic security framework to implement strategic security procedures, with the focus on end users, to ensure compliance with security policies and protection of vital resources.

CONTACT Sadaf Hina sadaf.hina@gmail.com

Aim of study

This review study aimed to synthesize the literature published from 2006 to 2016 to highlight the need for more exploration on information security policies' compliance (ISPC) in the HEI domain. This study has systematically reviewed and analyzed the available literature to gain an insight into the analytical theories and factors that significantly contribute to ISPC in the HEI domain. To analyze the results, this study focused on the frame and size of population samples undertaken in HEI studies. The study's second task was to investigate the difference in perceptions between technical and nontechnical respondents in these studies. To achieve the stated objectives, review protocols followed by[8,9] were incorporated. In its analysis of the literature, the study makes a novel contribution by suggesting an appropriate ISPC theory that is critical in the HEI domain.

Background

In its 2015 general incidents classification statistics, the Malaysian Computer Emergency Response Team (MyCert), Cyber Security, Malaysia, reported 9,915 incidents including cyber harassment, denial of service, fraud, intrusion, malicious codes, spam, and vulnerabilities. Moreover, spam email statistics were shockingly high with a total of 561,454 incidents. Such incidents commonly occur in organizations with employees falling victim due to their lack of awareness on how to deal with them.[10] The intrinsic and extrinsic motivators in information security behavior for ISPC can range from rewards to penalties.[11–13] Researchers have reported that major issues in noncompliant behavior include the lack of self-sustained knowledge[14] and ignorant behavior toward prescribed ISP roles and responsibilities. In their online survey among university employees, Chan and Mubarak[15] sought an understanding of the knowledge level of employees in an HEI, reporting that employees were unaware of the potential security threats, breaches, and preventive methods. These authors emphasized the significance of information security awareness (ISA) in HEIs to mitigate security risks and recovery costs.[15] In a similar study focusing on HEIs, Kam et al.[16] reported that ISPC behavior can be significantly improved through external pressures and forces. By applying neo-institutional theory, researchers validated the importance of regulative, normative, and cognitive external expectations for the enforcement of ISPs and awareness programs.[16] Like many other organizations, HEIs are implementing business plans to achieve corporate goals. Therefore, various factors that relate to employees' ISPC behavior need to be considered.

D'Arcy and Greene[17], in examining the effect of organizational culture on ISPC intentions, argued that organizations face noncompliance due to inadequate organizational, individual, and work environment factors. A challenge for organizations is to motivate employees to comply with the stipulated ISP rules and regulations. These researchers indicated that, regardless of whether intended or unintended, security breaches primarily originate from end users' lack of ISA and from complaints behavior.[17] Galvez et al.,[18] in their research, reported the factors that influence information security practices in organizations, deriving their constructs from the international standards in information security, ISO 17799/27002, which are considered as the code of practice. These authors explained individual information security practice at work by applying the social cognitive theory (SCT) constructs for information security. Their study suggested that, to achieve preventive security behaviors, organizations must follow practices based on international standards.[18]

The foremost need in building information security infrastructure in any organization is to realize and acknowledge the existence of threats. Critical energy infrastructure is considered the most vulnerable entity that must be protected under legitimate rules and regulations.[19] The information security of this type of infrastructure is addressed at the national level to prevent chaotic situations if a successful cyberattack occurs. Business organizations that significantly contribute to the national economy are often protected by authentic security protocols to mitigate the risks of financial and information loss.[20] The top management of vulnerable organizations must understand the necessity of information security and should vigilantly initiate security plans. With policy documents based on international standards, well-planned awareness programs, and regular monitoring, organizations can be led toward the development of a comprehensive ISC.[1,7,21,22]

Research methodology

Literature extraction

This study followed both an automated and manual search process to acquire as many published articles as possible to meet the defined objectives. These articles later went through rigorous filters to meet the study's inclusion criteria. Identified articles were then vigilantly analyzed to obtain reliable outcomes. Search queries were firstly made using keywords and phrases related to the literature under investigation. Secondly, reliable databases and search engines were enlisted to ensure the reliability and validity of the articles collected. Table 1 shows the queries (with keywords and phrases) generated for the search process.

As mentioned, this study also conducted some manual searches for related articles through search engines and reference lists of downloaded articles. The keywords and phrases were mapped onto articles downloaded from reliable databases and search engines listed in Table 2. The keywords, abstracts, and full text of downloaded articles were vigilantly explored using the identified phrases and keywords. In total, 200 articles were identified for use in validating the accuracy and consistency of the objectives under investigation. The basic inclusion criteria comprised English as the language of the article, academic significance, empirical data collection, peer-reviewed publication, and the field of ISPC in organizations/institutions.

Books, online magazines, white papers, industry reports and articles without methodological evidence were excluded from the literature synthesis.

Analysis of extracted literature

Studies incorporating systematic literature analysis should carefully assess the quality of publications included for

Table 1. Keywords and phrases with queries for literature search.

Keywords and phrases	Queries
Employees' security behavior ICT policies Information security management Information security maturity Information security policies compliance Information security policies Information systems security Information technology Organizational security culture Policies compliance Security culture Security policies	• "Information technology" AND "information security policies compliance" • "ICT policies and regulations" AND "universities" • ("Information security policies" OR "security policies" OR "policies") AND ("employees' behaviour" OR "behaviour" OR "attitude") • ("Employee" OR "employees" OR "user" OR "users" OR "staff") AND ("policy" OR "security policies" OR "policies compliance" OR "security compliance" OR "security behaviour") • ("Organization" OR "institution") AND ("information security policies") • ("Organization" OR "institution") AND ("security culture") • ("Organization" OR "institution") AND ("Malaysian") AND ("information security management" OR "maturity")

Note: ICT = information and communications technology.

Table 2. Databases and search engines used for literature search.

Databases and search engines	
Scopus	ACM Digital Library
AIS Electronic Library	Palgrave – Journals
IEEE	MIS Quarterly Journals
Science Direct	Web of Science
Emerald Insight – Information Management & Computer Security	Google Scholar (search engine)
ProQuest	Yahoo (search engine)
Springer	RefSeek (search engine)

review.[9] In the current study, the extracted articles were screened and discussed by the researcher and two domain experts. Publications with the same theoretical framework and, in their opinion, inconsequential differences were considered duplicates and excluded from the review process. Articles relying only on expert opinions and without methodological evidence were also excluded. After carefully exploring the literature for review, the articles were grouped according to the research objectives. As this research focused on ISPC, articles on diverse organizational settings were categorized as ISC, information security management (ISM) and ISA. The results were later analyzed to understand the extent within HEIs of information security maturity. The researcher intended

(1) to explore the significance of ISC and compliance;
(2) to explore the significance of ISA and compliance; and
(3) to explore the significance of ISM and compliance, particularly in HEIs.

Finally, 51 publications were extracted for further analysis, with the number of extracted articles and their year of publication shown in Table 3.

These publications were focused on effective ISC and compliance; ISM and compliance; ISPs and ISPC; behavioral intentions for information security; encouraging information security behavior through protection motivation; awareness and deterrence; assessment of ISC through awareness and training; and application and validation of multiple theories to better explain compliance and adherence with organizational policies.

Results analysis

ISC and compliance

An ISC can minimize and/or mitigate the risks to information assets as well as employees' intentional or unintentional malicious interactions with information assets and computing resources. The current research suggests that ISPC can be achieved at three levels by defining information security components that influence information security behavior, which, in turn, will cultivate ISC.[23] Hu et al.[24] believed that ISPC can be achieved if information security technology implementation is fully complemented with comprehensive ISA programs. These programs should comprise and convey a rigorous understanding of how individual, cultural, and organizational factors align in modeling individual behavioral intentions. In addition, the study highlighted the role of top management in being vigilant in defining organizational ISC.[24] It is believed that the implementation of a sound ISC can reduce the number of security breaches. An ISC is one in which the information security values and beliefs are shared by employees at all levels of the organization. It is considered as an important pillar in maintaining an adequate level of information security in organizations. It is suggested that security-conscious decision-making and security policy adherence can be influenced by cultivating a security culture. The literature has revealed various concepts and factors that contribute to thorough ISC application. Within ISC, D'Arcy and Greene[17] identified the factors of top management influence, security communication, and computer monitoring which, in turn, have a positive influence on security compliance intention. These researchers considered ISC as a multidimensional concept often addressed with a simpler approach.

AlHogail[25] presented the strategy, technology, organization, people, and environment (STOPE) design framework to address

Table 3. Number of articles extracted from publications.

Number of articles	03	04	01	04	06	02	09	04	07	09	02
Year of publication	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016

a wide set of issues related to human behavioral aspects to create a secure environment for information and communication assets. This researcher translated security issues into tasks based on the four main domains of the presented human factor diamond: preparedness, responsibility, management, and society and regulations. The research highlighted the need for change management principles that could guide the cultivation of ISC.[25] To foster and practice ISC, employees must understand their roles and responsibilities through some means of communication.

Chen and Wen[22] highlighted the importance of the three most vital factors, security policies, security programs, and security monitoring, in ISC development. These researchers validated their research model and showed the significant effect of security programs on ISC development. Their study findings showed that security monitoring influenced security culture unlike security policies, which showed a nonsignificant contribution toward security culture. This nonsignificant contribution was explained by stating that the mere existence of policies does not change employees' behavior.[22] Further evidence of this phenomenon was provided in a recent study with the researcher arguing that employees who read and understand ISPs contribute better to ISC.[7] The awareness of existing documents, that is, security policies, thus significantly contributes to security culture. Sherif et al.[21] presented an ISC framework based on a review of prior studies, indicating the substantial input of awareness, behavior, and culture in establishing security culture in organizations. Table 4 shows the authors, research methodologies, and findings in the areas of ISC and compliance.

The researchers in Table 4 have indicated the importance of security policies; rules and regulations; roles and responsibilities; security awareness; training; monitoring; and individual behavior to achieve thorough ISC in an organization. Research frameworks were empirically tested among technical and nontechnical respondents working in diverse organizational settings. Although the reported sample size in some studies was relatively low, justification took into account the sensitivity of the information security domain. It should be noted that none of these studies investigating ISC frameworks and assessments examined the HEI domain. Only partial responses were collected from HEIs for the validation of frameworks in some studies but nothing specific was reported on that domain. Conclusively, cultivating an ISC demands a comprehensive strategic plan incorporating the vision of top management in line with organizational security objectives in the form of security policies. These policies should then be periodically updated and disseminated. Finally, recurrent monitoring of acceptable and unacceptable behavior should be logged. However, these inferences still need to be rigorously inspected in the HEI domain.

Table 4. Summary of publications: information security culture and compliance.

Authors	Research methodology	Sample and size	Findings
Da Veiga and Eloff[23]	Quantitative method for validation of framework; structural equational modeling (SEM) for hypotheses testing	In total, 1085 employees from a South African audit and advisory firm	Clear guidance is given to management to design a strategic plan for cultivation of security culture within an organization.
Hu et al.[24]	Quantitative analysis for validation of research model based on top management, organizational culture, and theory of planned behavior (TPB) in organizations; SEM for hypotheses testing	Responses from 148 alumni of MIS and MBA programs of large public-sector university with administrative, operational, and IT job types in various industries	Role of top management in shaping employees' behavior for security compliance is emphasized.
D'Arcy and Greene[17]	Quantitative analysis for validation of research model based on security culture, job satisfaction, and perceived organizational support; partial least squares for hypotheses testing	In total, 127 responses were collected through online survey from technical and nontechnical employees in various industries.	Security culture was found to be a strong driver of employees' security compliance behavior in the workplace. Job satisfaction played a vital role in security intention.
AlHogail[25]	Expert opinion survey method used for analysis and validation of ISC framework based on STOPE (strategy, technology, organization, people, and environment) molded around human behavior	Nine information security experts participated in the study	The empirically tested framework can assist organizations in protecting valuable information assets by fostering appropriate ISC.
Chen and Wen[22]	Quantitative survey method incorporating SEM for the validation of framework	100 responses from four companies in US Midwest	Security education, training, and awareness program found to be the strongest predictor of security culture.
Da Veiga[7]	Quantitative case study approach (over 8 years) examining the influence of reading and nonreading of security policies on security culture through ISC assessment questionnaire	In total, 8,220 employees from a large organization operating in 12 countries participated at four intervals over the 8-year period	Findings emphasized that awareness of available ISPs significantly contributes to security culture.

ISM and compliance

The well-known phenomenon of ISM refers to the directing and regulation of the security of information assets possessed by organizations. It plays a vital role in enhancing organizational control over the flow of information within and external to the organization for business goals. For acceptable protection of information and computing resources, effective ISM requires

the implementation and maintenance of appropriate security controls, resources, and policies. However, information security issues have not always been the top priority of security professionals in organizations. In the past two decades, security professionals have started highlighting security breaches, such as email viruses, malware, software vulnerabilities, and internet worms, and have drawn attention to the role of top management support in dealing with security threats. Knapp et al.[26] investigated the influence of top management support on organizational security culture and security policy enforcement. These authors suggested that top management enforcement is critical to effectively address security problems, leading to effectual methods of building the understanding of security policies and security culture within organizations.[26] Security policy and policy compliance comprise a procedural system that requires vigilant and timely decisions by top management. Security implementation is costly and requires finance for technical controls (monitoring, etc.) and nontechnical controls (awareness programs, etc.). The literature has shown that investment in security controls is determined by the type and size of the industry. It can be postulated that the larger the business, the larger the vulnerabilities. For effective ISM implementation, Chang and Ho[27] highlighted the need for accurate organizational factors. Based on the ISO standard guidelines for ISM, the researchers designed and empirically validated a conceptual framework that provided tested factors for better ISM practices. A strong predictor of ISM was IT competence in an organization, with industry type and organizational size found to be positive determinants of ISM in organizations.[27] Therefore, ISM in HEIs cannot be overlooked.

In relation to ISM in HEIs, specific factors may be related to this domain's variant and open infrastructure. Ismail et al.[5] examined various security standards and frameworks including ISO, COBIT, MyMIS, and Committee of Sponsoring Organizations to present an information security framework that was HEI-specific. In line with the extant literature, their research emphasized the importance of available constructs and top management commitment to fulfill the security needs of HEIs.[5] In another study, ISM was encapsulated under organizational factors: the proposed framework depicted personal information security behavior as having a direct influence on compliance.[28] Padayachee[29] suggested that effective ISM by top management should regard end users and their perceptions on information security as essential aspects in developing a secure environment. It is argued that end users should be considered the focus of the information security concept. Effective ISM should minimize and/or mitigate potential security hazards at both technical and behavioral levels. Such practices can essentially improve employees' adherence to ISP.[29] Safa et al.[30] showed that diverse ISM strategies can achieve organizational ISP compliance. Their research framework established social bond theory (SBT) to understand end users' ISP compliance. Their research results suggested that appropriate management of information security knowledge (ISK) sharing within an organization can be done through intrinsic and extrinsic motivation. These arrangements can encourage employees to comply with ISP.[30]

Table 5 summarizes studies that empirically tested and validated the ISM factors and their contribution to compliance.

Most reviewed studies had a relatively smaller sample size, with surveyed respondents in most studies having a sound

Table 5. Summary of publications: information security management and compliance.

Authors	Research methodology	Sample and size	Findings
Knapp et al.[26]	Mixed-methods approach for validation of theoretical model; grounded theory and SEM technique were used	In total, 220 IS security professionals from 23 countries working in diverse industries participated in the quantitative study. A total of 68 certified information systems security professionals responded to the qualitative study through the online survey.	Top management can play a significant role in introducing a security culture in an organization and enforcing security policies' compliance for good practices.
Ernest Chang and Ho[27]	Quantitative method used to validate theoretical framework with multiple regression analysis technique	In total, 59 responses were collected from senior managers in various industries.	Organizational factors, such as IT competence, environmental uncertainty, industry type, and organization size have a significant influence on effectiveness of ISM.
Ismail et al.[5]	Mixed-methods approach for data collection; grounded theory and SEM technique for hypotheses testing	Four interviews conducted with IT personnel in 4 HEIs in Malaysia. In total, 72 questionnaires were used for quantitative data analysis.	The information security framework for HEIs includes specific factors, such as risk management, access control, ISP, awareness and training, and compliance.
Safa et al.[30]	Quantitative method and SEM technique used to validate theoretical framework and test hypotheses	In total, 462 questionnaires were used for analysis of data, acquired through online and self-administered data collection in four Malaysian companies.	Arrangements for information security knowledge sharing by top management increase end users' compliance with organizational ISPs.

technical background. The current study argues that ISC, ISM, and information security compliance should also be thoroughly and empirically assessed from the nontechnical end users' perspectives. Applying controls and enforcing policies by top management does not necessarily lead to information security compliance. The behavioral issues and knowledge deficiencies of employees need to be understood to overcome the gap between state-of-the-art controls and policies and employees' perceptions. Prior studies have defined ISM success factors as security practices, environmental influences, and organizational structure and culture.[31] Moreover, management practices play a significant role in IT and IS security.[32] Organizations have been advised in recent studies that they need to look at the diverse aspects of ISM that are responsible for comprehensive strategic plans; security education, awareness, and training programs; design and implementation of security policies; periodic monitoring; and human resource management to instigate information security compliance values.[8]

ISA and compliance

ISPs are regarded as the most important and crucial documents in effective information security implementation in organizations. Security policy documents are generally based on international standards for ISM (ISO/IEC 27002) and are molded according to organizational business objectives. Prior research has suggested the unique relationship between the strategic IS plan and corporate goals.[33] A vital part of ISM is defining and aligning its policies and plans with strategic plans. However, adherence with these security plans entirely depends upon end users, that is, employees. Therefore, the facts, causes, and influences of compliant and noncomplaint behavior need to be investigated. ISA has been found important in compliance within organizations. However, to acquire ISA and training program effectiveness, rich relevant resources of visual and textual material need to be incorporated. One empirical study highlighted that media richness has a positive and significant correlation with ISA.[34] The availability of online ISA programs can bring more users together, enabling either synchronous or asynchronous learning.[35] presented the results of an experimental research design using an intervention approach, which suggested that participation, the collective reflection of the participants and dialogue significantly improved the ISA of the intervention groups. Hence, periodic awareness programs conducted with focused groups can have a powerful impact in developing lasting knowledge on ISPC among employees. Another distinctive theory-based approach for an information security training (IST) program has been proved to develop goal-oriented and effective ISPC, with this action research intervention conducted by Puhakainen and Siponen[36] highlighting the need for continuous communication between employees.

Among organizations, HEIs have high revenue but are the least protected. In general, HEI employees are not motivated or encouraged to protect their institutions' tangible and intangible assets.[37] Ahlan and Lubis[6] suggested that the existence and awareness of ISPs in a university environment play a crucial role in protecting information assets. Results for the university under investigation showed a lack of risk management awareness. Their ISA model emphasized learning, adaptability, and performance factors related to the employee's role and responsibility.[6] In a similar study in an Australian HEI, researchers found that employees were generally lacking in ISA. In that study, it was suggested that ISA programs should be a part of risk assessment strategies in HEIs to foster ISPC.[15] Haeussinger and Kranz[38] believed that ISA could be developed through various means, with their study exploring and examining the factors that could influence the ISA of employees. The study also validated a comprehensive research model that presented institutional (ISPs, and security education, training, and awareness programs [SETA]); individual (ISK and negative experience [NEx]); and environmental (secondary sources influence [SSI], peer behavior [PEB]) antecedents of ISA leading to ISPC.[38] In organizations, ISA programs are designed to be conducted among employees with distinct areas of expertise and varied levels of technical knowledge. Information should be categorized so it can be delivered according to the ability of end users to receive it. Amankwa et al.[39] drew a thin line between information security education, IST, and ISA based on attributes, such as the focus, purpose, and method of delivery for each security procedure. Their study suggested that organizations could fit into any of the working definitions and emphases on the goals of security compliance.[39] An investigative study using the mixed-methods approach indicated that providing detailed ISA to employees on ISPs and procedures would have a positive impact on their attitude and behavior toward compliance.[40] Another empirical study integrated multiple theories (protection motivation theory [PMT][41] and the theory of planned behavior [TPB][42]) along with organizational factors and presented an information security-conscious care behavior (ISCCB) formation research model. Study findings have indicated that ISA is a strong and significant antecedent of employees' attitude toward information security behavior.[2] Researchers have argued that negligent behavior and lack of awareness of rules and regulations lead to destructive security breaches. Hence, ISA should be considered the most crucial element in ISPC achievement. Table 6 summarizes studies that empirically tested and validated ISA factors and their contribution to compliance.

Studies have conclusively suggested that ISA and training programs play a fundamental role in the acceptance of protective technologies, development of a security culture, and compliance with organizational policies. The diverse awareness programs can be adapted to match organizational needs. However, HEI employees are still lacking in their level of security awareness and compliance with institutional policies. A notable reason for this deficiency of knowledge in how to deal with security incidents is the absence of motivation for the protection of institutional assets.[43] Lack of understanding of their roles and responsibilities results in noncompliant behavior and security breaches among HEI employees. ISA is not merely the knowledge of potential security breaches or vulnerability but also an understanding of the available resources for reporting and receiving the response for addressing these risks. It is imperative that employees are aware of their roles and the rules and regulations as prescribed in their institutional security policies. Along with the provision of policies in HEIs, appropriate security education training and awareness programs are urgently needed. Moreover, periodic

Table 6. Summary of publications: information security awareness and compliance.

Authors	Research methodology	Sample and size	Findings
Shaw et al.[34]	An experimental research design methodology (pre- and post-tests, and post-tests) was used to test hypotheses.	In total, 153 university students from MIS course in Taiwan. All respondents had minimal ISA at the beginning of the study.	Effectiveness of each incorporated ISA program was highlighted for eventually improving security policies' compliance.
Albrechtsen and Hovden[35]	A mixed-methods approach in an experimental research design (pre- and post-tests) was used to test individuals' behavior.	In total, 197 participants from an organization.	Employees' participation, collective reflection and group discussions develop ISA and change individuals' behavior toward security policies' compliance.
Puhakainen and Siponen[36]	A mixed-methods approach in an experimental research design was used to test individuals' behavior.	In total, 16 respondents from a company.	In total, nine key findings were presented to improve ISA and training programs for ISPC.
Ahlan and Lubis[6]	A mixed-methods approach was used to evaluate relationships between variables.	In total, 306 respondents from the International Islamic University of Malaysia participated in the quantitative research design while randomly selected participants were used for the qualitative study.	When designing ISPs, ISA should be considered as the most vital element for effective ISPC.
Chan and Mubarak[15]	An exploratory research design was used to assess the security awareness level in an HEI.	In total, 308 responses were collected from the employees of a South Australian HEI.	The ISA level among HEI employees is generally lacking. Appropriate security awareness and training programs should be incorporated for enhanced compliance.
Haeussinger and Kranz[38]	A quantitative research design was used to test the hypothesized model.	In total, 475 responses were collected from employees from various industries.	Institutional (ISP, SETA); individual (ISK, NEx); and environmental (SSI, PEB) factors positively and significantly contribute to ISA that conclusively bring about ISPC.
Parsons et al.[44]	A mixed-methods approach was used to gauge ISA of employees. Web-based survey and interviews.	In total, 203 employees responded from three Australian organizations. Three interviews with senior management staff from each organization.	Information security knowledge of employees was found to be higher than their attitude and behavior towards compliance. Intense and periodic training programs are suggested to mold employees' behavior.
Safa et al.[2]	A mixed-methods approach was used to validate the hypothesized research model.	In total, 212 IS experts and IT professionals responded from Malaysian organizations.	Organizational factors significantly contributed to the TPB. The TPB and PMT significantly influenced ISCCB. However, perceived behavioral control could not explain significant variance in ISCCB.

Table 7. Key papers extracted from the literature.

Authors	Research methodology	Sample and size	Findings
Safa et al.[30]	An ISPC model based on social bond theory (SBT)	• Quantitative approach • 462 employees • Four companies in Malaysia	SBT (Sig) ®Attitude Attachment (Insig) ® ISPC Attitude (Sig) ® ISPC
Safa et al.[2]	An information security conscious care behavior (ISCCB) framework integrating PMT and the TPB with organizational factors (ISA, ISP, experience and knowledge)	• Mixed-methods approach • 212 employees • IS experts and IT professionals in Malaysia	Organizational factors (Sig) ® TPB TPB (Sig) ® ISCCB PBC (Insig) ® ISCCB PMT (Sig) ® ISCCB
Chen and Wen[22]	ISC framework	• Web-based survey • 100 employees • Four US Midwest companies	Security awareness + Monitoring (Sig) ® Security culture Security policy (Insig) ® Security culture
Humaidi and Balakrishnan[1]	Leadership style theory and health belief model	• Quantitative approach • 457 management personnel • Three local Malaysian hospitals	Transactional leadership style (Sig) ® ISA ISA (Sig) ® Compliance
Siponen et al.[45]	A multiple theory-based model incorporating PMT, the theory of reasoned action (TRA) and cognitive evaluation theory (CET)	• Quantitative approach • 669 employees • Corporations in Finland	PMT (Sig) ® ISPC. CET (Rewards) + PMT (response efficacy) (Insig) ® ISPC
D'Arcy and Greene[17]	Security compliance framework	• Quantitative approach • 127 computer professionals • Organizations in Mid-Atlantic region, USA	Top management + Monitoring + Awareness strategies (Sig) ® Security culture Security culture + Job satisfaction (Sig) ® ISPC Perceived organizational support (Insig) ® ISPC
Ifinedo[46]	A multiple theory approach integrating TPB, SBT, and social cognitive theory (SCT)	• Quantitative approach • 124 business managers and IS professionals • Canadian organizations	Socio-organizational factors (Sig) ® Attitudes (Sig) ® ISPC Subjective norms (Sig) ® ISPC SCT (Sig) ® ISPC
Haeussinger and Kranz[38]	An ISPC framework	• Quantitative approach • 475 employees • Various industries	Institutional + Individual + Environmental (Sig) ® ISA ISA (Sig)® ISPC
Bulgurcu et al.[11]	A comprehensive ISP compliance framework integrating (RCT) and (TRA)	• Quantitative approach • 464 respondents • Diverse organizations in USA	ISA (Sig) ® Outcome beliefs (Sig) ® Beliefs about compliance

monitoring of end users to amplify the response rate against security breaches will also motivate ISPC by employees.

Summary of the literature

Culture brings the required norms into a day-to-day routine and, following the accepted custom, conveys the habitual pattern of compliance. The literature has confirmed that the ISC developed in organizations can reduce the risk of security breaches and potential incidents, as compliance with rules and regulations becomes a habit.[47] The development of a sound ISC in HEIs still requires the exploration of factors that could encourage compliance with ISPs. ISM is generally associated with the involvement of top management and security managerial practices.[1,48] However, the extant studies have called for improvement and a more holistic approach from the managerial point of view to achieve better ISPC.[8]

Table 7 summarizes the key literature extracted from the studies under review. The theoretical frameworks, methodology, and main findings from all domains of ISC, ISM, and ISA highlight the research gap in the area of ISPC in HEIs.

The investigation of the presented theories, in the light of the detailed literature review, has suggested that none of the theories have been systematically and thoroughly tested, and particularly not in any HEI. The samples for ISPC research are generally taken from among professionals working in large-scale organizations. Although these studies have presented various significant factors, the influence of institutional governance in protection motivation for employees to comply with institutional policies has never been examined. The literature has described HEI employees as the least concerned, motivated, and aware of the potential threats that can harm their personal and work computing environment. Hence, a hybrid and precise governance framework that can motivate employees toward the protection of assets and ISPC is a crucial need in HEIs. SETA, and the monitoring and provision of policies have been found as substantial components of institutional governance in building an ISC. PMT is established as an exceptional ISPC predictor. When dealing with the protection of information assets, personal experience should also be considered. The significant key factors from the validated theories should be integrated, tested, and validated in the HEI context in future research.

Conclusion

HEIs are growing in terms of contemporary technologies, infrastructure, and research activities. Business processes in these institutions are closely interconnected with human resources and information security elements. Their employees are the end users of security plans and risk management procedures. Extant research has shown that HEIs continue to struggle with applying effective ISM and practices. These high-revenue businesses are the least secure due to their isolated security strategies and plans. The alignment of security procedures with business strategies is still a task that many HEIs have yet to achieve. The awareness of the "dos" and "don'ts" in an organization leads to smoothly functioning procedures and practices. As a complete bundle of knowledge, ISA should provide focused education and training for ISPC achievement. The association of ISA with compliance in HEIs is confirmed in prior studies. However, the influence of ISA programs, with respect to comprehensive institutional governance, in enhancing motivation for the protection of assets and resulting in ISPC is yet to be empirically tested. Awareness of these plans and procedures is the first and foremost step in achieving better IS security. Additional technical controls for physical and virtual threat restrictions are vital regulators of potential security threats. These regulators should be periodically upgraded for improved monitoring of tangible and intangible assets. State-of-the-art HEIs are generally set up with an efficient response team to deal with security attacks and recovery procedures. However, end users are usually unaware of this response efficacy and hence repeatedly remain victims of malicious attacks. Therefore, providing detailed, yet understandable, ISPs; focused ISA programs; and periodic monitoring procedures are the crucial elements of comprehensive institutional governance. Conclusively, this can bring about motivation to protect institutional assets and achieve compliance with institutional rules and regulations.

Limitations and future work

Although rigorous approach was adopted to search appropriate and adequate literature for this review study, there is still a chance for some unspotted literature that could add to enhance the purpose of the study. To further understand ISPC among HEI employees and to present evidence from the literature review, the researcher will empirically investigate the relationship of PMT and the sources of knowledge with the TPB. A comprehensive research framework will therefore be designed by extracting latent and observed variables from validated theories to empirically test and validate the research framework. This study also suggests looking at information security policies compliance issues in less anticipated organizations.

Acknowledgments

This research is endorsed by Computer and Information Sciences Department, Universiti Teknologi PETRONAS (UTP), Malaysia.

Notes on contributors

Sadaf Hina is a postgraduate student and PhD candidate at Universiti Teknologi PETRONAS, Malaysia. Her research interest is in information security, security policies development and compliance, social media, security in social networks, and potential usage of social media in education. She has worked as a research officer under the Exploratory Research Grant Scheme, funded by the Malaysian Government. Her primary effort has been to explore the factors affecting the school-based adoption of social networking sites for participation/collaboration among school stakeholders. She has published in various leading journals with distinguished indices.

Dr. P. Dhanapal Durai Dominic is currently an associate professor in Universiti Teknologi PETRONAS, Malaysia. He received his PhD in Management at Alagappa University, India. He received his Post-Graduate Diploma in Operations Research from Pondicherry University, India; Masters of Business Administration; Masters of Philosophy in Mathematics and Masters of Science in Mathematics from Bharathidasan University, India. He has been working in the capacity of editorial board member for renowned journals. His research

interests include Management Information Systems and Knowledge Management. He has published in several journals with high-impact factors and distinguished indices like SCOPUS and ISI.

References

1. Humaidi N, Balakrishnan V. Leadership styles and information security compliance behavior: the mediator effect of information security awareness. Int J Inf Educ Technology, Articles Adv. 2015;5(4):311–18. doi:10.7763/IJIET.2015.V5.522.
2. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Computers & Security. 2015;53:65–78. doi:10.1016/j.cose.2015.05.012.
3. Willison R, Warkentin M. Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly. 2013;37(1):1–20. doi:10.25300/MISQ.
4. Siponen M, Pahnila S, Mahmood A. Employees' adherence to information security policies: an empirical study. new approaches for security, privacy and trust in complex environments. Springer; 2007. p. 133–44.
5. Ismail Z, Masrom M, Sidek Z, Hamzah D. Framework to manage information security for Malaysian Academic Environment. Inf Assur Cybersecurity. 2010;2010:1–16.
6. Ahlan AR, Lubis M. Information security awareness in university: maintaining learnability, performance and adaptability through roles of responsibility. 2011 7th International Conference on Information Assurance and Security (IAS), IEEE; 2011 Dec 5–8; Melacca, Malaysia.
7. Da Veiga A. The influence of information security policies on information security culture: illustrated through a case study. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015); 2015 Jul 1–3; Lesvos Greece. Lulu. com.
8. Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: a literature review. Int J Inf Manage. 2016;36(2):215–25. doi:10.1016/j.ijinfomgt.2015.11.009.
9. Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf Manag Comput Security. 2014;22(1):42–75. doi:10.1108/IMCS-08-2012-0045.
10. Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst. 2009b;18(2):106–25. doi:10.1057/ejis.2009.6.
11. Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 2010;34(3):523–48. doi:10.2307/25750690.
12. Son J-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf Manag. 2011;48(7):296–302. doi:10.1016/j.im.2011.07.002.
13. Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst. 2009a;47(2):154–65. doi:10.1016/j.dss.2009.02.005.
14. Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: its influence on end users' information security practice behavior. Computers & Security. 2009;28(8):816–26. doi:10.1016/j.cose.2009.05.008.
15. Chan H, Mubarak S. Significance of information security awareness in the higher education sector. Int J Comput Appl. 2012;60(10):23–31. doi:10.5120/9729-4202.
16. Kam H-J, Katerattanakul P, Gogolin G, Hong S. Information security policy compliance in higher education: a neo-institutional perspective. *PACIS*. 2013.
17. D'Arcy J, Greene G. Security culture and the employment relationship as drivers of employees' security compliance. Inf Manag Comput Security. 2014;22(5):474–89. doi:10.1108/IMCS-08-2013-0057.
18. Galvez SM, Shackman JD, Guzman IR, Ho SM. Factors affecting individual information security practices. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, ACM; 2015 Jun; Newport Beach, CA, USA.
19. Onyeji I, Bazilian M, Bronk C. Cyber security and critical energy infrastructure. Electricity J. 2014;27(2):52–60. doi:10.1016/j.tej.2014.01.011.
20. Al-Omari A, El-Gayar O, Deokar A. Security policy compliance: user acceptance perspective. International Conference on 2012 45th Hawaii System Science (HICSS), IEEE; 2012 Jan 4–7; Maui, HI, USA.
21. Sherif E, Furnell S, Clarke N. Awareness, behaviour and culture: the ABC in cultivating security compliance. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE; 2015 Dec 14–16; London, UK.
22. Chen Y, Wen K-W. Impacts of comprehensive information security programs on information security culture. J Comput Inf Syst. 2015;55(3):11–19. doi:10.1080/08874417.2015.11645767.
23. Da Veiga A, Eloff JH. A framework and assessment instrument for information security culture. Computers & Security. 2010;29(2):196–207. doi:10.1016/j.cose.2009.09.002.
24. Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis Sci. 2012;43(4):615–60. doi:10.1111/deci.2012.43.issue-4.
25. AlHogail A. Design and validation of information security culture framework. Comput Human Behav. 2015;49:567–75. doi:10.1016/j.chb.2015.03.054.
26. Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information security: management's effect on culture and policy. Inf Manag Comput Security. 2006;14(1):24–36. doi:10.1108/09685220610648355.
27. Ernest Chang S, Ho CB. Organizational factors to the effectiveness of implementing information security management. Ind Manag Data Syst. 2006;106(3):345–61. doi:10.1108/02635570610653498.
28. Furnell S, Rajendran A. Understanding the influences on information security behaviour. Computer Fraud & Security. 2012;2012(3):12–15.
29. Padayachee K. Taxonomy of compliant information security behavior. Computers & Security. 2012;31(5):673–80. doi:10.1016/j.cose.2012.04.004.
30. Safa NS, Von Solms R, Furnell S. Information security policy compliance model in organizations. Computers & Security. 2016;56:70–82. doi:10.1016/j.cose.2015.10.006.
31. Norman AA, Yasin NM. Information systems security management (ISSM) success factor: retrospection from the scholars. European Conference on Information Warfare and Security, Academic Conferences International Limited; 2012 Jul; Laval, France.
32. Phillips B. Information technology management practice: impacts upon effectiveness. J Organ End User Comput. 2013;25(4):50–74. doi:10.4018/JOEUC.
33. Doherty NF, Fulford H. Aligning the information security policy with the strategic information systems plan. Computers & Security. 2006;25(1):55–63. doi:10.1016/j.cose.2005.09.009.
34. Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Computers & Education. 2009;52(1):92–100. doi:10.1016/j.compedu.2008.06.011.
35. Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security. 2010;29(4):432–45. doi:10.1016/j.cose.2009.12.005.
36. Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: an action research study. MIS Quarterly. 2010;34(4):757–78. doi:10.2307/25750704.

37. Rezgui Y, Marks A. Information security awareness in higher education: an exploratory study. Computers & Security. 2008;27(7):241–53. doi:10.1016/j.cose.2008.07.008.
38. Haeussinger F, Kranz J. Information security awareness: its antecedents and mediating effects on security compliant behavior. Security and Privacy of Information and IS; 2013; Milan, Thirty Fourth International Conference on Information Systems.
39. Amankwa E, Loock M, Kritzinger E. A conceptual analysis of information security education, information security training and information security awareness definitions. 2014 9th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE; 2014 Dec 8–10; London, UK.
40. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security. 2014a;42:165–76. doi:10.1016/j.cose.2013.12.003.
41. Rogers RW, Cacioppo JT, Petty R. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. Social psychophysiology: A sourcebook; 1983. p. 153–77.
42. Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process. 1991;50(2):179–211. doi:10.1016/0749-5978(91)90020-T.
43. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computers & Security. 2012;31(1):83–95. doi:10.1016/j.cose.2011.10.007.
48. Tu Z, Yuan Y. Critical success factors analysis on effective information security management: a literature review. Information Systems Security, Assurance, and Privacy Track (SIGSEC), Twentieth Americas Conference on Information Systems; 2014; Savannah
44. Parsons K, McCormac A, Pattinson M, Butavicius M, Jerram C. A study of information security awareness in Australian government organisations. Inf Manag Comput Security. 2014b;22(4):334–45. doi:10.1108/IMCS-10-2013-0078.
45. Siponen M, Mahmood MA, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inf Manag. 2014;51(2):217–24. doi:10.1016/j.im.2013.08.006.
46. Ifinedo P. **Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition**. **Inf Manag**. 2014;**51**(1):69–79. **doi**:10.1016/j.im.2013.10.001.
47. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Inf Manag. 2012;49(3):190–98. doi:10.1016/j.im.2012.04.002.