Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Information security cultural differences among health care facilities in Indonesia

Puspita Kencana Sari [a,b,*], Adhi Prasetio [a], Candiwan [a], Putu Wuri Handayani [b], Achmad Nizar Hidayanto [b], Syaza Syauqina [a], Eka Fuji Astuti [a], Farisha Pratami Tallei [a]

[a] *Faculty of Economics and Business, Telkom University, Bandung, Indonesia*
[b] *Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia*

ARTICLE INFO

Keywords:
Health information management
Health information system
Information security culture
Health care
Health care facilities

ABSTRACT

Background: Health information security (IS) breaches are increasing with the use of information technology for health care services, and a strong security culture is important for driving employees' information asset protection behavior.

Objective: This study aimed to analyze differences in information security cultures (ISCs) across health care providers based on factors drawn from the ISC model.

Methods: We used twelve factors to measure the ISCs of health care providers. This research applied a survey method with the Kruskal–Wallis H Test and the Mann–Whitney U Test as data analysis techniques. We collected the data through a questionnaire distributed to 470 employees of health care facilities (i.e. hospitals, community health centers, and primary care clinics) in Indonesia.

Results: The results revealed the differences between health care provider types for 9 of the 12 security culture factors. Top management support, change management, and knowledge were the differentiating factors between all types of health care providers. Organizational culture and security compliance only differed in primary care clinics. Meanwhile, security behavior, soft issues and workplace independence, information security policies, training, and awareness only differed in hospitals.

Conclusion: The results indicated that each type of health care provider required different approaches to develop an ISC considering the above factors. They provided insight for top management to design suitable programs for cultivating ISCs in their institutions.

1. Introduction

Health information is one of the most important factors for providing good health services. To administer medical treatment, medical personnel must refer to the patient's medical history, which includes information about the patient's condition, such as allergies and previous treatment history. The patient's medical history must be kept confidential according to the regulations governing the protection of personal data; therefore, health care providers have a responsibility to maintain the confidentiality, availability, and integrity of patient health information [1, 2, 3]. The health industry has recently experienced more data breaches than other sectors [4] and increased risk due to the use of cloud, big data, Internet of things (IoT), and other technologies [5]. According to Statista, there were 525 data breaches in the United States in 2019 for the medical/health care industry—more than for the educational (113), banking/financial (108), and government/military sectors (83) [6].

Technical incidents are the main cause of data breaches in health care, followed by unauthorized access or disclosure incidents [7, 8]. A major reason for security breaches in health care systems is the fact that personal health information (PHI) is more valuable than other personal identification information [4]. PHI is health information in any form, including health records (physical, electronic, or verbal), health histories, laboratory test results, and medical bills with individual identifiers [9]. PHI can be used to profit from the victims' medical conditions and make fake insurance claims, allowing the purchase and resale of medical equipment [10], threatening data confidentiality. Data availability can be compromised by malware attacks [5], causing problems for critical hospital procedures. The main purpose of PHI data security is patient safety and privacy [11]. Data security is important for increasing patients'

* Corresponding author.
E-mail address: puspitakencana@telkomuniversity.ac.id (P.K. Sari).

https://doi.org/10.1016/j.heliyon.2021.e07248
Received 24 July 2020; Received in revised form 17 November 2020; Accepted 3 June 2021

trust [2, 12] and is also an influential factor for user acceptance of health referral systems that facilitate communication and standardization between health facilities [13]. Since data security is crucial, an organization needs to manage its information security (IS) effectively.

The objective of IS management is to ensure organizational sustainability and minimize losses [14] by protecting the confidentiality, integrity, and availability of information [15, 16] through various controls. One of the most important security controls is the delivery of IS awareness programs, which ensure that system users are aware of security risks and understand related information security policies (ISPs) and procedures [17]. An organization, as a system owner, is responsible for providing qualified IS personnel and general controls [18]. Supported by security knowledge, information systems can foster good security behavior.

IS behavior evolves to become an organizational behavior that fosters an ISC as an expansion of the organizational culture [19]. Previous research [19] addressed the determinants and consequences of controlling user security behavior and reviewed the development of an IS awareness culture that changed the organizational culture and strengthened it through ISPs. Significant security gains were accomplished by enhancing the organization's security culture [20], including improving the patient care delivered by health care providers [3]. The aim of establishing an ISC is to encourage employees' and stakeholders' adherence to the organization's ISPs [1]. ISC can be defined as the perceptions, attitudes, assumptions, beliefs, values, and knowledge of employees or stakeholders when interacting with organizational systems and processes, with the aim of protecting information assets and influencing security behavior to ensure compliance with policies and controls [20, 21]. Since ISC is an expansion of an organization's culture [19, 20], embedding the expected culture depends on each organization's condition, which is influenced by many factors; therefore, it is vital to understand the factors that can contribute to the success of ISC.

This research investigated health care providers in Indonesia. Health care organizations have specific cultures that make IS implementation more challenging, such as communication and trust issues [22], data ownership issues [23], and the different professional values and norms of employees [24]. The Indonesian government has promoted health and medical data integrity through a national referral system [13]; hence, IS focuses on ensuring the confidentiality, integrity, and availability of data managed by various health care organizations.

A health care facility is a place that carries out individual promotive, preventive, curative, and rehabilitative health care interventions mandated by the government and/or society as defined in the Ministry of Health Regulation (No. 71 of 2013) regarding health services and national health insurance. Article 2 in this Regulation divides health care facilities into two types: first-level health facilities and advanced referral health facilities. First-level facilities include community health centers, private practitioners, dentists, primary care clinics or equivalent, and small hospitals. Advanced referral facilities include main clinics or their equivalents, general hospitals, and special hospitals. Health care is carried out in stages according to medical needs, starting with the first-level facilities. If a patient requires advanced treatment based on medical indications, the patient must be referred to the closest referral facility.

Empirical studies relating specifically to ISC in health care facilities are still rare. More studies have discussed IS behavior and compliance, which are the expected results of ISC. A literature review [25] concluded that a research gap regarding IS in a health care context necessitates further studies to determine what creates an ISC in organizations. Recent studies compared IS climates among four categories of health care professionals [26], but they did not conduct the comparison at an institutional level. This research aims to fill the gap in the empirical research concerning IS cultures in a health care context. Moreover, organizational influences are significant factors in security protection, since a data security culture, combined with organizational policies, procedures, and management, can act as a powerful defense against data breaches [27]. Previous research on ISCs in health care contexts [28] only took hospitals as their study subjects and did not cover other types of health care organizations, which might have different approaches to ISC. Therefore, the goal of this study was to enhance understanding of ISCs and their contributing factors in many types of health care organizations with different characteristics. Furthermore, by identifying the different factors influencing ISCs in health care facilities, the study highlighted different ways of enhancing ISCs to protect health information for each institution. This research contributes to the literature by investigating ISCs in the three types of health care institutions that have not yet been covered by previous research.

Based on these problems, the research question for this study was: “How do IS cultures differ across different types of health care facilities?” For health care facilities as system owners, this research is expected to provide insights for developing an ISP and program to cultivate ISC. For the Indonesian government as the regulator, the outcomes of this research are expected to provide lessons learned for the development of supporting regulations for nationwide e-health establishments.

After presenting the research problems, objectives, and motivations in the Introduction, this paper is organized into the following six sections. The first section discusses the research hypotheses. The second section describes the research method. The third and fourth sections sequentially explain the research results and the interpretation of our findings. The fifth section considers the research limitations, and the last section provides the conclusions of our research.

2. Research hypotheses

This study used some factors drawn from the ISC model developed by previous researches [28, 29, 30, 31, 32]. Those studies were selected due to their completeness in defining ISC factors. Furthermore, literature reviews conducted by Alnatheer [29], Sherif et al. [30] and Nasir et al. [32] identified some success factors for ISC cultivation extracted from many previous studies. The main factors were senior management support, effective ISPs, IS awareness, IS training and education, IS risk analysis and assessment, IS compliance, organizational culture, IS behavior, information asset management, change management, trust, user security management, leadership, and governance. The empirical research conducted by Da Veiga and Martins [31] revealed some factors of ISCs and IS subcultures in various types of organizations in Australia and South Africa, including health care providers. Those factors were information asset management, IS management, change, user management, ISPs, trust, IS leadership, training and awareness, privacy, and IS programs. Meanwhile, a study by Hassan and Ismail [28] focused specifically on health care organizations (including hospitals) in Malaysia and found some success factors for ISC, namely security behavior, security awareness, security value, and the enforcement of ISPs. For this research, we adopted 12 variables for ISC factors from Da Veiga and Martins [31] since this was the most complete and current empirical research we found during the research period. Figure 1 shows the conceptual framework that we adopted from Da Veiga and Martins. Their study took as its research subject a global bank operating in various countries; however, most respondents came from South Africa, which is a developing country like Indonesia. Based on the country's characteristics, Da Veiga and Martins' study resembled the current research. IS in health care has the same level of urgency as in banking, where the value of confidentiality, availability, and data integrity is extremely high. Health care organizations contain various subcultures [33], as do global banks; therefore, the results of Da Veiga and Martins' research were adopted for this study. This research used 12 variables drawn from Da Veiga and Martins as shown in Figure 1.

Top management roles in organizations are critical for shaping a desired culture [31], and such roles were frequently mentioned in previous studies as success factors for cultivating organizational cultures, including security cultures [32]. Top management support refers to the degree to which top management understands the significance of IS and its involvement in IS operations [29]. A corporate ISP should define the

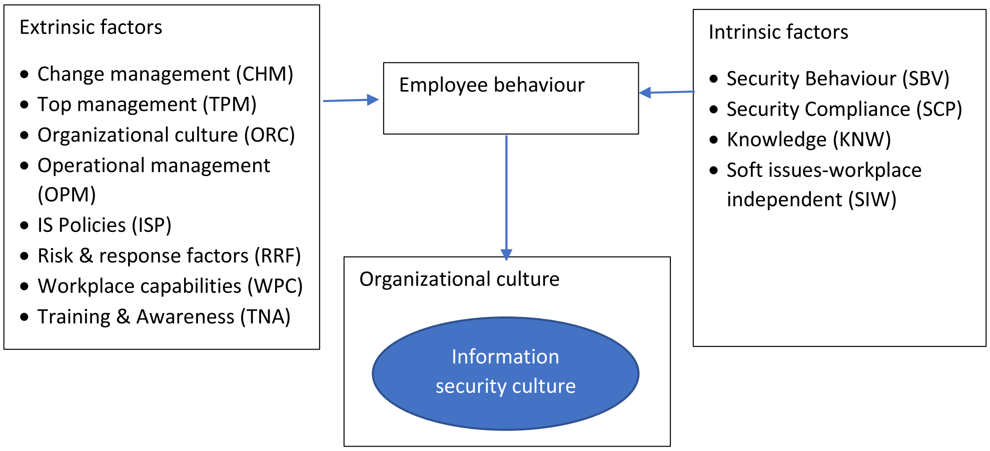
Extrinsic factors
• Change management (CHM)
• Top management (TPM)
• Organizational culture (ORC)
• Operational management (OPM)
• IS Policies (ISP)
• Risk & response factors (RRF)
• Workplace capabilities (WPC)
• Training & Awareness (TNA)
Employee behaviour
Intrinsic factors
• Security Behaviour (SBV)
• Security Compliance (SCP)
• Knowledge (KNW)
• Soft issues-workplace independent (SIW)
Organizational culture
Information security culture

Figure 1. Conceptual Framework adapted from Da Veiga and Martins [31].

leadership's IS vision and objectives [30]. Since different types of organizations may have different security visions and objectives, top management support may also differ:

H1. There are differences in top management support across different types of health care providers.

The security requirements of an organization influence the strength of controls over policies and procedures in the workplace regarding how the organization tolerates actions by individuals [34]. Such tolerance is reflected in some organizational capacities, including system usability, employee turnover, employees' skills and tracking procedures, task importance, security practices, disciplinary procedures, achievements, and rewards, and these capacities can affect security culture [31]. They also influence employees' personalities and further affect their security behavior [35]. Since different types of organizations can have different procedures and practices for managing employees, workplace capabilities can also vary:

H2. There are differences in workplace capabilities across different types of health care providers.

ISC is recognized as an efficient means of promoting an organization's safe conduct and managing safety hazards [32]. The way in which organizations identify, prevent, detect, and react to safety events affects the ISC [31]. By conducting security risk analysis and evaluation, organizations and employees can be made aware of the damage they can do to security and develop a security-conscious culture [29]. Since different types of organizations can implement risk analysis and mitigation in different ways, risk response factors may also vary:

H3. There are differences in risk response factors across different types of health care providers.

Based on a risk assessment strategy, organizations can take a thorough approach to managing and governing IS and ensure proper leadership, reviews, auditing, and tracking to help maintain a positive ISC [31]. Security management and operations have also been mentioned in previous research as important for fostering an ISC [32]. Since different organizations might have different approaches to managing their IS, security operational management approaches may also differ:

H4. There are differences in operational management across different types of health care providers.

Change management procedures should support technology changes and help the staff to integrate and accept the changes so that they become part of the culture. Changing an organization's technology can improve security, quality, effectiveness, and reliability, which have important effects on information functionality, usability, privacy, and security [31]. Change management has often been mentioned in previous studies as a success factor for IS along with management commitment and leadership [32], and different organizations might have different approaches to managing technology changes in their organizations:

H5. There are differences in change management across different types of health care providers.

Organizational cultural factors affect how information is processed and protected and how they ultimately affect the ISC, since the free flow of information, openness, and transparency are maintained in some organizations but restricted in others [31]. Organizational culture refers to shared trends in employee conduct in companies, and the connection between the organizational culture and ISC is comparable to other notions of culture, but varies in practice (in terms of symbols, heroes, and rituals) [30]. The development of an ISC includes social, cultural, and ethical interventions meant to enhance organizational members' security-related conduct and is regarded as an organizational subculture [29]. Since different organizations can have different codes of conduct for managing their employees' behavior, their organizational cultures may also differ:

H6. There are differences in organizational culture across different types of health care providers.

Individuals have certain IS knowledge, developed implicitly and explicitly, enabling them to comply with security regulations, and that knowledge affects how data is processed and IS controls are used [31]. IS knowledge is usually required when work tasks have to be performed in accordance with excellent data security practices [30]. An efficient ISC relies on employees understanding IS [20, 32]. Since each employee may have different knowledge and each organization has unique security practices, security knowledge (KNW) may also differ:

H7. There are differences in security knowledge across different types of health care providers.

The workforce's understanding of ISPs and procedures has a beneficial effect on their attitude toward ISPs and compliance, resulting in adherence as a noticeable characteristic in an organization with a strong and healthy ISC [31]. A powerful connection between employees' security culture, compliance with security, and extra-role security behavior demonstrates the importance of complying with security policies for establishing ISCs and improving security in organizations [29]. Since each organization can have a different ISP and their employees have different intentions to follow it, security compliance (SCP) might also differ:

H8. There are differences in security compliance across different types of health care providers.

Security controls affect employees' interaction with data resources, and they consequently display security behavior, the goal of which is to protect data assets based on the policies of the organization [31]. An ISC stimulates employees' appropriate security conduct and compliance, and the cultivation of an ISC can therefore help to minimize or prevent security breaches [30]. Security behavior is the key criterion to be highlighted in an ISC, and the employees' behavior, although important, can differ because they tend to do what they feel good about [28]. Since each employee can behave differently, their security behavior can also be different:

H9. There are differences in security behavior across different types of health care providers.

Soft employee problems, such as real-life exposure to threat, security-related incidents, media coverage, private interests, group/community interests and consciousness, policy recognition, skills, etiquette, engagement, obedience, self-disapproval, and morality, can affect the ISC [31]. Employees' personalities, including their experiences of security incidents, affect their behavior toward security policies and practices inside an organization and further influence the security culture [30, 36]. Since every employee might have different personality problems, soft issues and workplace independence (SIW) can also differ:

H10. There are differences in soft issues and workplace independence across different types of health care providers.

To have a beneficial effect, IS awareness and training must be undertaken to inform employees about data risks, the appropriate checks to use, and the policies to follow in an ISC [31]. Concerning hospital information system users, training should highlight the awareness that needs to be creatively embedded in the staff [28]. Based on previous research, security training and awareness have become important factors for organizations in cultivating their ISCs [29, 30, 32]. Since organizations often have different training programs and their employees have different awareness, training and awareness may also differ:

H11. There are differences in training and awareness across different types of health care providers.

An ISP is a critical cornerstone for directing an ISC and creating a base of shared values and beliefs [31]. Previous studies have defined it as a key factor in cultivating a security culture [29, 30, 32]. IS in health care systems must distinguish between the privacy and security controls that the organization must emphasize, such as the security policy [28]. Since health care providers can have different viewpoints regarding security controls, their ISPs can also differ:

H12. There are differences in information security policies across different types of health care providers.

Each variable we used consisted of three indicators, so there were 36 indicators in total. The 12 variables, their definitions, and their indicators are summarized in Table 1. A questionnaire was developed based on the indicators drawn from previous studies as adopted in the hypotheses.

3. Research methods

The sample for this study consisted of employees of health care providers in Indonesia, especially in Bandung city, which is the capital of the West Java Province and has the biggest total population of all the provinces (48.68 million people in 2018) [38,39]. Health care providers as research subjects were limited to state-owned community health centers (CHCs) and privately owned primary care clinics (PCCs) as representatives of first-level health care facilities, and hospitals as representatives of advanced referral health care facilities. According to the Indonesian National Health Insurance System, health facilities can be classified into first-level health facilities and advanced referral health facilities. First-level health facilities consist of PCCs, CHCs, private doctors' clinics, and private dental clinics, while referral health facilities consist of main clinics, hospitals, pharmacies, and opticians. However, according to the Regulation of the Minister of Health No. 9 of 2014, main clinics and PCCs are classified as clinics. Based on their service scopes, PCCs only provide basic medical services, while main clinics can provide both basic and specialist medical services. Both types of clinics have similar service scopes: providing outpatient, inpatient, one-day care, and emergency services. According to Regulation of the Minister of Health No 43 of 2019, CHCs only provide basic medical services and focus on public health services in a specified community. Hospitals can provide a wider range of services, including basic and specialist medical services and medical support services (such as radiology, laboratory analysis, rehabilitation, etc.) and non-medical services such as the disposal of corpses. We distinguished CHCs and PCCs as different types of research subjects since they have different characteristics. CHCs are owned by the district government, so they are more strictly regulated and their employees are civil servants with long-term work contracts. Meanwhile, PCCs are mostly owned by private organizations that develop their own policies, are less strictly regulated, and usually give their employees short-term work contracts. Therefore, in this research, we only considered hospitals, PCCs, and CHCs as research subjects. The sample consisted of 100 PCCs, 78 CHCs, and 30 hospitals operating in Bandung city. All those providers were initially invited to participate in this research, but not all of them responded. A purposive sampling technique was used, with the sampling of data sources conducted according to certain criteria. The criteria specified health facilities that had implemented information systems in their operational activities and had given their permission to be used as research subjects.

The data collection process took about three months from December 2018 to February 2019. First, we requested a research permission letter from the government office that had the appropriate authority (i.e., Bakesbangpol). We then obtained licenses from related government offices with license numbers as follow: 070/034/Bakesbangpol (for hospitals); 070/2444/Bakesbangpol (for CHCs); 070/2443/Bakesbangpol (for PCCs). Initially, we targeted at least five respondents from each health care facility—a specialist, a general practitioner (doctor/dentist), a nurse/midwife, an administrator, and the IT manager. We submitted our proposal to all PCCs, CHCs, and hospitals in Bandung, of which only 25 PCCs (with a response rate of 25%), 22 CHCs (28%), and 9 hospitals (30%) met the criteria and agreed to participate in the research. Since only nine hospitals responded to our proposal, we contacted more respondents from each health care facility.

Data collection was conducted through hard-copy questionnaires distributed directly to the respondents in the selected health care providers. The questionnaire used closed questions with five alternative answers, scored using a 5-point Likert scale ranging across levels of agreement and disagreement (1 = totally disagree to 5 = totally agree). The items in the questionnaire (Appendix A) were derived from indicators used in previous research [28, 29, 30, 31], as seen in Table 1. Each indicator became one item in the questionnaire, which had a total of 36 items consisting of three items per variable. Also, seven demographic questions and one filter question asking about the existence of an ISP were included in the questionnaire. Before the questionnaire was used, validity and reliability tests were conducted to confirm that all the statements in the questionnaire could be easily understood by the respondents and that the questionnaire could be used as a research instrument. The tests were conducted using IBM SPSS Statistics 25 for Windows software. Validity and reliability tests were carried out for 30 health care provider employees in Indonesia (from random areas). The validity test used the Pearson product-moment correlation to consider the correlation score and compare it with the score from the r critical value table. Table 2 summarizes the correlation scores for the validity test and the Cronbach's alphas for the reliability test. It shows that all the items in the questionnaire were valid because each item had an r product moment greater than the r table (0.361); therefore, all the items could be used to measure the research variables. The reliability test for all the variables in Table 2 showed that all the Cronbach's alpha

Table 1. List of research variables, definitions, and indicators.

Variables/Factors	Definition	Code	Indicators
Top management support (TPM) [29, 30, 31, 32]	Top management commits to supporting IS in the organization and communicating its views to the employees.	TPM1	Top management demonstrates its commitment to IS.
		TPM2	Top management considers IS to be important.
		TPM3	Top management explains what is expected of employees regarding IS.
Workplace capabilities (WPC) [31]	The organization has the capability to foster an ISC for all stakeholders by establishing policies, procedures, and practices as IS controls.	WPC1	There is a non-disclosure agreement in the employment contract to prevent information leaks.
		WPC2	Disciplinary action is taken against anyone who does not follow the ISP.
		WPC3	IS systems are maintained regularly so that system outages can be avoided.
Risk and response factors (RRF) [29, 31, 32]	The organization applies risk management to IS management, including risk analysis, risk mitigation, risk evaluation, and communication.	RRF1	The organization conducts a risk analysis to provide a risk evaluation before deciding an action.
		RRF2	The organization mitigates risks to reduce the impact of an event that has the potential to or has been harmful.
		RRF3	The organization provides information about regulations relating to IS along with their sanctions.
Operational management (OPM) [31, 32]	The organization conducts adequate management, reviews, auditing, and tracking to help guide a favorable ISC.	OPM1	The organization periodically reviews the information system used.
		OPM2	The organization conducts external/internal audits of the information system used.
		OPM3	Every contract with third parties, especially relating to IT, includes items regarding IS.
Change management (CHM) [31, 32]	Change management procedures are integrated into information system changes to help staff integrate and accept change and become part of the ISC.	CHM1	The organization changes work practices to ensure the security of information assets.
		CHM2	Changes to IS systems (for example, regularly changing passwords, making backup files) secure important information.
		CHM3	Employees are willing to improve work practices and protect information assets.
Organizational culture (ORC) [29, 30, 31]	The organization ensures its employees have the knowledge, skills, and commitment to support information asset protection.	ORC1	Employees have knowledge of IS.
		ORC2	Employees have the required skills to keep information safe.
		ORC3	Employees demonstrate a commitment to IS.
Knowledge (KNW) [20, 30, 31, 32]	The organization's employees have the appropriate knowledge to ensure IS.	KNW1	Employees understand the importance of protecting personal, sensitive, and confidential information.
		KNW2	Employees understand the negative consequences of IS problems.
		KNW3	Employees know the IS authorities in the organization.
Security compliance (SCP) [29, 31]	The organization encourages its employees to follow security policies and procedures.	SCP1	The leader communicates clear directions about protecting information to employees or third parties.
		SCP2	Employees follow the IS procedures/policies established by the organization.
		SCP3	Employees are aware of their role in IS, but do not necessarily fully follow current practices.
Security behavior (SBV) [28, 30, 31]	The organization's employees exhibit behavior that supports good security controls.	SBV1	Employees do not leave sensitive/confidential information in unsecured places.
		SBV2	Employees regularly check documents for malware infections.
		SBV3	Employees consider the negative consequences of their work before posting anything on social network sites.
Soft issues and workplace independence (SIW) [30, 31, 37]	The organization's employees understand the consequences of security breaches since they have personal experience.	SIW1	Employees realize that if an IS problem occurs, it can have adverse effects.
		SIW2	Employees use antivirus software because they know the consequences of not using it.
		SIW3	Employees are aware that outside interference can change orientation and commitment regarding ISPs.
Training and awareness (TNA) [28, 29, 30, 31, 32]	The organization's staff know that IS training can improve their awareness to prevent security incidents.	TNA1	Employees believe there is a need for additional training in using IS controls to protect information.
		TNA2	Employees believe in effective IS awareness initiatives.
		TNA3	Employees are aware that training in recognizing and reacting to social attacks gives good results.
Information Security Policies (ISPs) [28, 29, 30, 31, 32]	The organization establishes security policies applicable to and understandable by its employees	ISP1	ISPs in the organization can be applied in daily work.
		ISP2	Employees fully understand the ISPs of the organization.
		ISP3	Employees believe practical ISPs should be implemented.

values were approximately 0.7, thus indicating that all the items were reliable.

The measurement tool for this research used factors adapted from Da Veiga and Martins [31]. The research employed a quantitative method with multivariate data analysis. Since no variable was described as independent or dependent, we used interdependence techniques to analyze the data, such as variance analysis [40]. We employed two statistical procedures to compare unrelated samples: the t-test for independent samples for parametric testing and its non-parametric testing equivalent Mann–Whitney test. We tested the data normality first to decide which method should be used to analyze the data. If the data followed a normal distribution, we would use the parametric procedure; otherwise, we would use a non-parametric procedure [41] that was not based solely on parameterized families of probability distribution [42].

Table 2. Validity test and reliability test results.

Variable	Cronbach's Alpha	Indicator	Pearson Correlation
TPM	0.856	TPM1	0.607
		TPM2	0.369
		TPM3	0.505
WPC	0.774	WPC1	0.424
		WPC2	0.666
		WPC3	0.656
RRF	0.882	RRF1	0.593
		RRF2	0.617
		RRF3	0.666
OPM	0.719	OPM1	0.649
		OPM2	0.691
		OPM3	0.627
CHM	0.704	CHM1	0.534
		CHM2	0.714
		CHM3	0.473
ORC	0.919	ORC1	0.637
		ORC2	0.698
		ORC3	0.698
KNW	0.725	KNW1	0.446
		KNW2	0.754
		KNW3	0.633
SCP	0.719	SCP1	0.503
		SCP2	0.467
		SCP3	0.681
SBV	0.789	SBV1	0.741
		SBV2	0.623
		SBV3	0.698
SIW	0.770	SIW1	0.74
		SIW2	0.537
		SIW3	0.662
TNA	0.825	TNA1	0.41
		TNA2	0.636
		TNA3	0.608
ISP	0.832	ISP1	0.641
		ISP2	0.827
		ISP3	0.655

The normality test using Kolmogorov–Smirnov analysis showed that not all the data were normally distributed, as shown in Table 3. Since some data did not meet the normality assumption test (asymptotic significance value less than 0.05), we used a non-parametric statistical procedure—the Kruskal–Wallis test—to compare more than two independent samples, followed by Mann–Whitney post-hoc testing to spot the differences in the perceptions of ISC factors across the three types of health facilities. We referred to previous research by Alimohammadi et al. [43] and Fernández-Alemán et al. [44], who used the same statistical methods (i.e., the Kruskal–Wallis test and the Mann–Whitney U test). The Kruskal–Wallis test is a ranking-based non-parametric test that aims to determine whether there are statistically significant differences between two or more groups of independent variables affecting the dependent variables [41]. The Kruskal–Wallis test was not able to tell us which group was significantly different; only that there were at least two groups that differed significantly. Since we had three groups, further post-hoc tests were performed using the Mann-Whitney U test to explore which groups were different.

Table 3. Asymptotic significance values (Kolmogorov-Smirnov).

Variables	PCC	CHC	HOS
TPM	0.000	0.000	0.000
WPC	0.000	0.001	0.000
RRF	0.000	0.000	0.000
OPM	0.000	0.001	0.001
CHM	0.000	0.001	0.000
ORC	0.000	0.000	0.002
KNW	0.000	0.001	0.000
SCP	0.000	0.000	0.000
SBV	0.000	0.000	0.000
SIW	0.000	0.000	0.000
TNA	0.000	0.000	0.002
ISP	0.000	0.000	0.000

4. Results

Data were collected from 470 respondents (150 from PCCs, 154 from CHCs, and 166 from hospitals). The respondents were mainly female (67%), aged 19 to 29 (49%), and with undergraduate degrees (44%). Most respondents (60%) were health workers (general practitioners, specialists, dentists, nurses, midwives, and pharmacists), and the rest were non-health workers (managers, administrators, receptionists, and IT staff). This distribution aligned with the data from the Central Bureau of Statistics [45], according to which the health care sector is dominated by female workers and most workers (75%) are health workers [46]. All the health care facilities that became research subjects had established policies relating to IS. Figure 2 depicts the demographics of the study respondents.

Table 4 depicts the descriptive statistics for each factor in each health care provider. Across all types of providers, the variable with the highest value was knowledge. This also applied to primary health care facilities, namely PCCs and CHCs. Meanwhile, the variables with the highest scores in hospitals were soft issues and workplace independence. The average score for ISC factors was highest in PCCs, followed by CHCs and hospitals in that order. The Kruskal–Wallis test results can be seen in Table 5. The next step was the Mann–Whitney U test to identify further differences in the results of the Kruskal–Wallis test for each factor that had an asymptotic significance value < 0.05. Table 6 shows the asymptotic significance values for the results of the Mann-Whitney U test across health facilities. If the value was <0.05, there was a difference between the first and second facility types.

5. Discussion

Based on the results of the Kruskal–Wallis test (Table 6), the three types of health care facilities had the same characteristics for workplace capabilities, risk response factors, and operational management. This indicated that CHCs, PCCs, and hospitals had similar capabilities to foster ISC for all their stakeholders by establishing policies, procedures, and practices as IS controls. Risk management, including risk analysis, risk mitigation, risk evaluation, and communication, were applied by health care facilities to IS controls. Risk analysis and assessment had a strong influence on the ISCs because they helped organizations to become aware of losses and damage [29]. Furthermore, adequate management, reviews, auditing, and tracking based on the risk assessment helped to ensure a favorable ISC [31] across all the health care facilities. This result meant that our hypotheses about workplace capabilities, risk response factors, and operational management were not supported. As mentioned in Section 2, workplace capabilities relate to how organizations deal with their employees' actions [33]. Since most health care facilities focus on patient treatment practices, they were expected to tolerate their employees' IS errors similarly. This could affect risk response factors in the health care facility itself, since the ways in which they identify, prevent, detect, and react to security events [31] affect their tolerance of security threats. Meanwhile, an organization's operational management is also affected by a risk assessment strategy that helps to maintain a positive security culture [31].

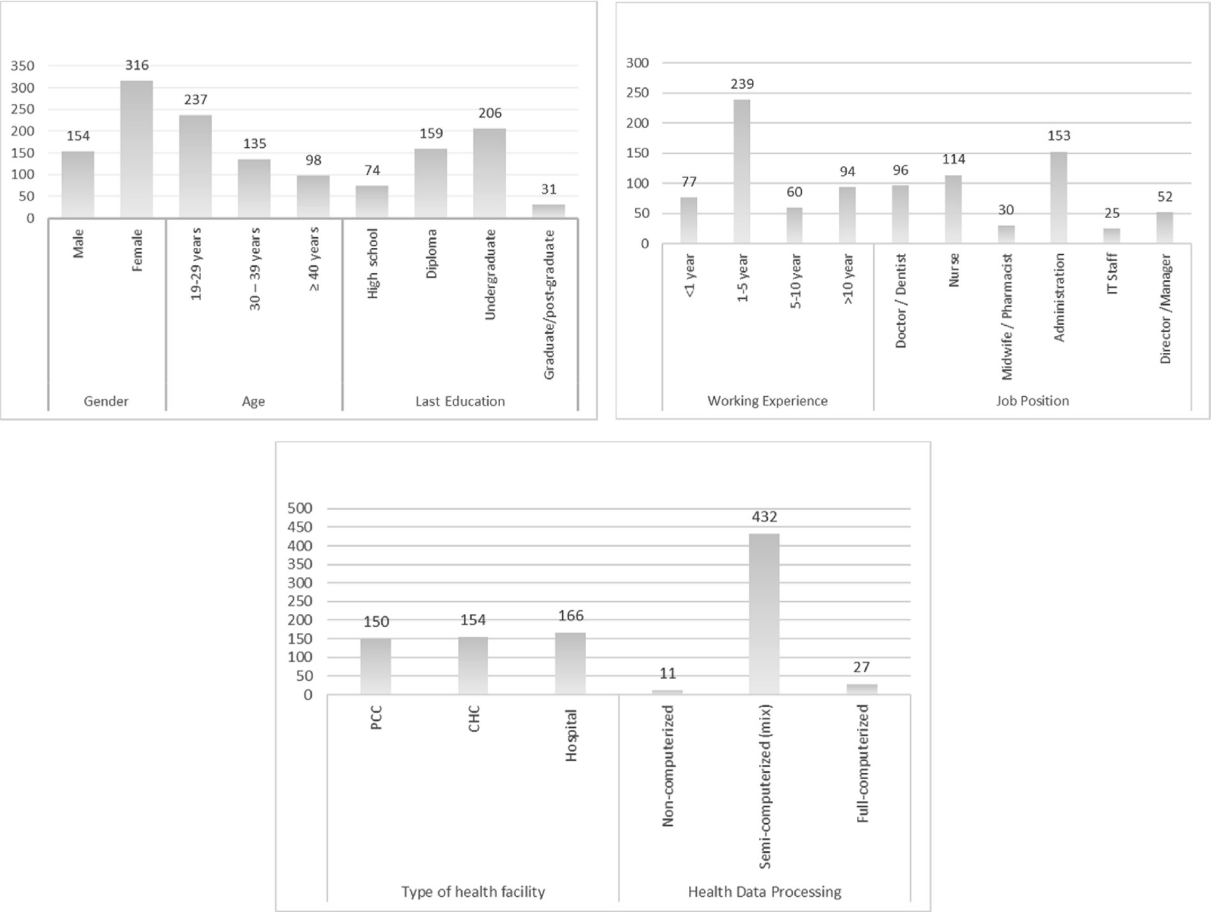

Figure 2. Respondent demographics.

Nowadays, risk management is considered in international standards, such as quality management standards (e.g., ISO 9001:2015) or IS management standards (ISO 27001:2018). This factor could be influenced by other factors, particularly workplace capabilities and operational management; for example, if an organization had conducted risk analysis and risk evaluation before deciding on a risk response (RRF1), it involved a non-disclosure agreement in employment contracts to prevent information leaks (WPC1). It also depended on contracts with third parties, primarily IT contracts, always including IS provisions (OPM3). Furthermore, based on risk assessment, all the PCCs, CHCs, and hospitals could accept the same level of risk because they had the same levels of tolerance. This relationship implied that risk response factors, workplace capabilities, and operational management had the same characteristics. Based on this consideration, we determined that all risk response factors, workplace capabilities, and operational management indicators had a significant relationship and the same features for these health care facilities.

These three types of health care facilities had different characteristics for other factors. Top management support, change management, and

Table 4. Descriptive statistics test.

Variables	Mean Value			
	PCC (N = 150)	CHC (N = 154)	Hospital (N = 166)	Total (N = 470)
TPM	12,560	12,844	11,843	12,400
WPC	11,900	11,786	11,801	11,828
RRF	12,027	11,526	11,506	11,679
OPM	12,020	11,877	11,548	11,806
CHM	12,213	12,468	11,476	12,036
ORC	12,300	11,682	11,133	11,685
KNW	12,760	13,169	11,922	12,598
SCP	12,313	11,838	11,277	11,791
SBV	12,493	12,701	11,735	12,294
SIW	12,660	12,714	11,976	12,436
TNA	12,573	12,604	11,898	12,345
ISP	12,480	12,097	11,596	12,043
Total	12,358	12,275	11,643	12,078

Table 5. Results of the kruskal–wallis test.

No	Information Security Factors	Asymp. Sig	Conclusion
1	Top Management (TPM)	**0.000***	Different among healthcare provider types
2	Workplace Capabilities (WPC)	0.999	No-difference among healthcare provider types
3	Risk Response Factors (RRF)	0.239	No-difference among healthcare provider types
4	Operational Management (OPM)	0.220	No-difference among healthcare provider types
5	Change Management (CHM)	**0.000***	Different among healthcare provider types
6	Organizational Culture (ORC)	**0.000***	Different among healthcare provider types
7	Knowledge (KNW)	**0.000***	Different among healthcare provider types
8	Security Compliance (SCP)	**0.000***	Different among healthcare provider types
9	Security Behaviour (SBV)	**0.003***	Different among healthcare provider types
10	Soft Issue–workplace independent (SIW)	**0.018***	Different among healthcare provider types
11	Training and Awareness (TNA)	**0.009***	Different among healthcare provider types
12	Information Security Policies (ISP)	**0.003***	Different among healthcare provider types

[*] Asymp. Sig. > 0.05 indicates that there were differences across health care provider types.

knowledge differed across health care facilities, proving the hypotheses of this study (i.e H1, H5, and H7) as illustrated in the previous section. Based on the post-hoc Mann-Whitney U test, top management support in PCCs, CHCs, and hospitals had different ways of demonstrating their commitment to IS due to consideration of different levels of importance. Most previous studies agreed that top management has a great influence on the establishment of ISCs in organizations [29]. This was comparable to change management factors, which also had different properties for modifying and improving work procedures to ensure the security of data resources and improve data asset security in PCCs, CHCs, and hospitals. It is important to consider the integration of change management and knowledge management in cultivating an ISC [20]. The current research showed that each type of health care facility had a different level of knowledge. PCCs, CHCs, and hospitals varied in understanding the importance of protecting personal, sensitive, and confidential information and the negative consequences of IS problems.

Hospitals and CHCs had the same characteristics in terms of organizational culture and security compliance. In state-owned health facilities, operational and managerial policies in CHCs are strongly regulated by the government. Hospitals can be state- or privately owned, but their establishment and operations are also strictly controlled by government regulations. CHCs and hospitals provide more services, including

Table 6. Results of the mann-whitney U test.

ISC Factors	Mean Rank			Asymp. Sig.	Conclusion
	PCC	CHC	Hospital		
TPM	142.19	162.54	-	**0.037***	Each type of facility is different.
	170.87	-	147.32	**0.019***	
	-	182.40	140.18	**0.000***	
CHM	141.26	163.44	-	**0.023***	Each type of facility is different.
	169.20	-	148.83	**0.042***	
	-	181.22	141.27	**0.000***	
ORC	167.23	138.15	-	**0.003***	Hospital and CHC are same, but PCC is different.
	179.95	-	139.12	**0.000***	
	-	169.13	152.49	0.102	
KNW	137.54	167.07	-	**0.002***	Each type of facility is different.
	173.65	-	144.81	**0.004***	
	-	189.84	133.28	**0.000***	
SCP	165.61	139.73	-	**0.007***	Hospital and CHC are same, but PCC is different.
	178.39	-	140.53	**0.000***	
	-	169.77	151.90	0.078	
SBV	146.59	158.25	-	0.229	PCC and CHC are same, but hospital is different.
	169.14	-	148.88	**0.043***	
	-	178.37	143.92	**0.001***	
SIW	149.81	155.12	-	0.585	PCC and CHC are same, but hospital is different.
	169.72	-	148.36	**0.033***	
	-	174.31	147.69	**0.009***	
TNA	149.42	155.50	-	0.525	PCC and CHC are same, but hospital is different.
	171.04	-	147.17	**0.018***	
	-	174.96	147.08	**0.006***	
ISP	158.70	146.46	-	0.200	PCC and CHC are same, but hospital is different.
	176.02	-	142.67	**0.001***	
	-	171.00	150.76	**0.046***	

[*] Asymp. Sig. < 0.05 indicates that the ISC factor differed.

outpatient, inpatient, surgery, pharmacy, laboratory, and other services. Since PCCs do not provide inpatient, surgery, or laboratory services, this might have caused them to have different organizational cultures. Since their top management support and security knowledge also had different characteristics, it affected their security compliance. This aligned with previous research conducted by Humaidi and Balakrishnan [47] revealing that, in Malaysian public hospitals, management support had an indirect effect on user security compliance.

PCCs and CHCs had the same characteristics in terms of security behavior, soft issues, training and awareness, and ISPs, but they differed from the ones in hospitals. Based on the size of the organization, PCCs and CHCs were similar to one another but not to hospitals. Because of PCCs' and CHCs' smaller size, their employees might have more homogeneous behavior than those in hospitals. Employees have different behaviors when dealing with sensitive information, malware infections, and the sharing of information on social network sites. Since security behaviors are influenced by organizational security policies and awareness programs [19], those two groups of health care facilities had different characteristics for both factors. Hospitals might have more complex IS threats and vulnerabilities due to their health care service coverage; for example, hospitals provide more services than other health care facilities, including medical support services (such as radiology, laboratory, and rehabilitation services) and non-medical services. Some of these services require additional medical devices and systems that need to be integrated with other systems, which increases security threats, such as interference with the radiology/laboratory system's bridging to the hospital information system. Also, possible vulnerabilities include backdoors in the systems or devices. Hospitals therefore have more extensive ISPs and programs for training and awareness. In terms of soft issues and workplace independence, the employees have different understandings of what it means in case of an IS issue, which can cause adverse effects, and they may use antivirus software because they understand the implications of not using it. Additionally, employees are conscious that external interference can alter the direction and application of ISPs.

Figure 3 illustrates the IS factor difference model. This model shows the overall position of each ISC factor derived from the results regarding PCCs, CHCs, and hospitals. Based on Table 5, workplace capabilities, risk response factors, and operational management had significant values of 0.999, 0.239, and 0.220, respectively. These findings suggested that those factors did not have significant differences according to health care organization types. The other factors had significant differences across health care organization types based on the following significant values in Table 5: top management support (0.000), change management (0.000), organizational culture (0.000), knowledge (0.000), security compliance (0.000), security behaviors (0.003), soft issues and workplace independence (0.018), training and awareness (0.009), and ISPs (0.003). Furthermore, based on the significant values from the Mann-Whitney U test in Table 6, we found that:

- Top management support, change management, and knowledge exhibited significant differences across the three organization types.
- Security behaviors, soft issues and workplace independence, training and awareness, and ISPs exhibited no differences between CHCs and PCC, but significant differences between CHCs and hospitals, and between PCCs and hospitals.
- Organizational culture and security compliance exhibited no differences between CHCs and hospitals, but significant differences between hospitals and PCCs and between CHCs and PCCs.

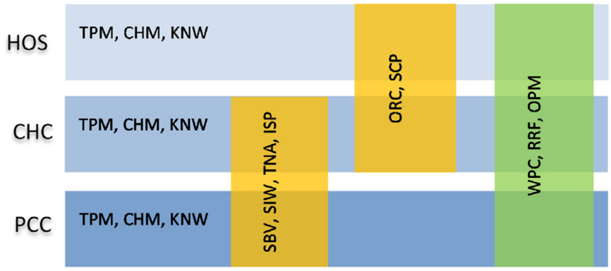

Figure 3. ISC factors difference model.

This study has some implications. In terms of theoretical implications, these results complete the Da Veiga and Martins [31] study by comparing ISCs in different organization types. They also enrich the Nasir et al. [32] literature review with other factors, such as soft issues, workplace independence, and organizational culture. This study enhances research on ISCs in health care provider organizations dominated by hospitals by exploring ISC factors in small health care facilities such as clinics. We found that some factors were similar for every type of health care facility, but others were different for every type. The study also revealed that hospitals and CHCs were similar for some factors, but they were not similar to PCCs. Further study is needed to determine whether the factors of ISC are influenced by the scale of services offered and the levels of regulation governing the organizations.

In terms of practical implications, the results of this study are expected to provide information to help managers of health facilities determine the right IS protection programs, specifically for ISC. Health care facilities with similar ISC factors can follow ISPs and practices adopted by other facilities as best practices. However, for other factors, health facilities need to develop different procedures and guidelines so that ISCs can be successfully cultivated. The government could also consider these factors in the formulation of IS policies for health care provider organizations, according to their respective conditions.

As seen in the ISC factor different model (Figure 3), each factor that influences an ISC can be different for one health care facility, but the same for another. This implies that the enhancement of ISCs may need a similar or different approach depending on the factor; for example, based on previous research [44] in health care facilities, factors that remained low were workplace capabilities, training and awareness, security behaviors, and ISPs. The current study implies that every health care facility can use a similar approach for workplace capabilities, such as non-disclosure agreements in employment contracts, disciplinary action, and regular IS systems maintenance. According to Soomro et al. [48], IS management has a more important role than IT professionals regarding IS responsibility. Based on our research, the top management and change management factors had different influences on ISC for each type of health care facility. This implies that a different approach should be used for each health care facility. However, operational management was similar across health care facilities, so we believe that a similar approach could be adopted, such as reviewing the IS used, conducting internal/external audits, and maintaining IS systems regularly. Furthermore, according to Deursen et al. [49], traditional IS risks such as sharing passwords and losing assets were more frequent occurrences than outsourcing or new technology such as cloud computing. Based on our research, there was no difference between health care provider types for the risk response function factor. This implied that all health care provider types can use similar approaches for risk analysis, mitigating risks, and providing information about IS, along with relevant sanctions for breaches.

6. Limitations

This research has some limitations since the influence of the ISC factors on IS effectiveness in health care provider organizations was not measured and compared. The study also did not measure the importance of those factors for ISCs in organizations. Furthermore, the indicators of ISC in this research were not specific to any particular technology implementation. New or future technology utilization in health care facilities, such as the Internet of Things, big data, or robotics, might result in different security cultures.

7. Conclusion

Some ISC factors differed across CHCs, PCCs, and hospitals, and some did not. Workplace capabilities, risk response factors, and operational management were similar for all health care facilities. Top management, change management, and knowledge were the factors that differed for each type of facility. Organizational culture and security compliance only differed for PCCs, while the remaining factors only differed for hospitals. This indicated the importance of employing different approaches for each type of health care to enable them to develop ISCs that consider those different influential factors.

Declarations

Author contribution statement

P. K. Sari, A. Prasetio, Candiwan: Conceived and designed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

P. W. Handayani, A. N. Hidayanto: Analyzed and interpreted the data; Wrote the paper.

S. Syauqina, E. F. Astuti, F. P. Tallei: Performed the experiments.

Funding statement

This work was supported by the Basic and Applied Research Grant Scheme (grant number No. 052/PNLT3/PPM/2018), Telkom University, Indonesia.

Data availability statement

Data will be made available on request.

Declaration of interests statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

Acknowledgements

This study received licenses from the National Unity and Politics Agency, West Java Province, Indonesia, with the following license numbers: 070/034/Bakesbangpol (for hospitals); 070/2444/Bakesbangpol (for CHCs); 070/2443/Bakesbangpol (for PCCs).

Appendix A. Questionnaire Items and Construct

1. Top management support (TPM)
   - TPM1: Top management demonstrates a commitment to information security.
   - TPM2: Top management considers information security to be important.
   - TPM3: Top management explains what is expected from employees regarding information security.
2. Workplace capabilities (WPC)
   - WPC1: There is a non-disclosure agreement in the employment contract to prevent information leaks.
   - WPC2: The disciplinary procedure is taken against anyone who does not comply with the information security policy.
   - WPC3: Information security systems are managed regularly so that system outage can be avoided.
3. Risk and response factors (RRF)
   - RRF1: The organization has conducted a risk analysis to provide a risk evaluation before deciding.
   - RRF2: The organization mitigate risks to reduce the impact of a potentially or already harmful event.
   - RRF3: The organization provides information about regulations related to information security along with their sanctions.
4. Operational management (OPM)
   - OPM1: The organization periodically reviews the information system used.
   - OPM2: The organization conducts an external/internal audit to review the information system used.
   - OPM3: Every cooperation agreement with third parties, especially related to IT, always includes items to maintain information security.
5. Change management (CHM)
   - CHM1: Organizations make changes in work practices to ensure the security of information assets.
   - CHM2: Changes to information security systems (for example, regularly changing passwords, making backup files) are needed to secure important information.
   - CHM3: Employees are ready to improve work practices to be better at implementing information asset security.
6. Organizational culture (ORC)
   - ORC1: Employees have knowledge of information security.
   - ORC2: Employees have good work skills to keep information safe.
   - ORC3: Employees demonstrate a commitment to information security.
7. Knowledge (KNW)
   - KNW1: Employees understand the importance of protecting personal, sensitive, and confidential information.
   - KNW2: Employees know the negative consequences of information security problems.
   - KNW3: Employees know the authorities in information security in the organization.
8. Security compliance (SCP)
   - SCP1: The leader communicates clear directions on how to protect information to employees or third parties.
   - SCP2: Employees follow the information security procedures/policies established by the organization.
   - SCP3: Employees are aware of their role in information security, but do not necessarily fully comply with current practices.
9. Security behaviour (SBV)
   - SBV1: Employees do not leave sensitive/confidential information in unsecured places.
   - SBV2: Employees regularly check documents to anticipate malware infections.
   - SBV3: Employees consider the negative consequences of their work before posting anything on social networking websites.
10. Soft issues – workplace independent (SIW)
    - SIW1: Employees realize that if an information security problem occurs, it can have adverse effects.
    - SIW2: Employees use antivirus software because they know the consequences of not using it.
    - SIW3: Employees are aware outside interference can change orientation and commitment regarding information security policies.
11. Training and awareness (TNA)
    - TNA1: Employees believe there is a need for additional training to use information security controls to protect information.
    - TNA2: Employees believe in effective information security awareness initiatives.
    - TNA3: Employees are aware that training to recognize and react to social attacks gives good results.

12. Information security policies (ISP)
    - ISP1: Information security policies in the organization can be applied in daily work.
    - ISP2: Employees understand the information security policies of the organization easily.
    - ISP3: Employees believe practical information security policies should be implemented.

References

[1] D. Box, D. Pottas, A model for information security compliant behaviour in the healthcare context, Procedia Technol. 16 (2014) 1462–1470.

[2] I.T. Agaku, A.O. Adisa, O.A. Ayo-yusuf, G.N. Connolly, Concern about security and privacy , and perceived control over collection and use of health information are related to withholding of health information from healthcare providers, J. Am. Med. Inf. Assoc. 21 (2014) 374–378.

[3] L. Coventry, D. Branley, Cybersecurity in healthcare: a narrative review of trends, threats and ways forward, Maturitas 113 (March) (Jul. 2018) 48–52.

[4] C. for I. Security, Data Breaches: in the Healthcare Sector, www.cisecurity.org, 2018 [Online]. Available: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/. (Accessed 3 December 2018).

[5] S. Schick, Security Breaches in Healthcare: 70 Percent of Organizations Hit Globally, Report Shows, securityintelligence.com, 2018 [Online]. Available: https://securityintelligence.com/news/security-breaches-in-healthcare-70-percent-of-organizations-hit-globally-report-shows/. (Accessed 20 December 2018).

[6] J. Clement, Number of Data Breaches in the United States from 2013 to 2019, by Industry, Statista, 2020 [Online]. Available: https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/. (Accessed 11 November 2020).

[7] HIPAAJournal, Analysis of 2018 Healthcare Data Breaches, www.hipaajournal.com, 2019 [Online]. Available: https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/. (Accessed 20 January 2019).

[8] Y.A. Setyoko, R. Yasirandi, Security protection profile on smart card system using ISO 15408 case study: Indonesia health insurance agency, in: 6th International Conference on Information and Communication Technology, ICoICT), 2018.

[9] HIPAAJournal, What Is Considered PHI under HIPAA? www.hipaajournal.com, 2017 [Online]. Available: https://www.hipaajournal.com/considered-phi-hipaa/. (Accessed 20 December 2018).

[10] W. Ashford, Most Healthcare Organisations Have Been Breached, Report Shows, www.computerweekly.com, 2018 [Online]. Available: https://www.computerweekly.com/news/252436215/Most-healthcare-organisations-have-been-breached-report-shows. (Accessed 20 December 2018).

[11] M. Masrom, A. Rahimly, "Overview of data security issues in hospital information systems, Pac. Asia J. Assoc. Inf. Syst. Online 7 (4) (2015) 51–65.

[12] T. Glenn, S. Monteith, "Privacy in the digital world: medical and health data outside of HIPAA protections, Curr. Psychiatr. Rep. 16 (2014) 494.

[13] P.W. Handayani, I.R. Saladdin, A.A. Pinem, F. Azzahro, A.N. Hidayanto, D. Ayuningtyas, Health referral system user acceptance model in Indonesia, Heliyon 4 (12) (2018), e01048, 1–33.

[14] H. Kruger, L. Drevin, T. Steyn, A vocabulary test to assess information security awareness, Inf. Manag. Comput. Secur. 18 (5) (2010) 316–327.

[15] R.C. Mitchell, et al., Corporate information security management, New Libr. World 100 (5) (1999) 213–227.

[16] M. Paryasto, A. Alamsyah, B. Rahardjo, Big-data security management issues, in: 2nd International Conference on Information and Communication Technology, ICoICT), 2014, pp. 59–63.

[17] H.A. Kruger, W.D. Kearney, A prototype for assessing information security awareness, Comput. Secur. 25 (4) (2006) 289–296.

[18] T.R. Peltier, Information Security Fundamentals, second ed., Routledge, 2014.

[19] D. Box, D. Pottas, Improving information security behaviour in the healthcare context, Procedia Technol. 9 (2013) 1093–1103.

[20] A. Alhogail, A. Mirza, Information security culture: a definition and a literature review, in: 2014 World Congress on Computer Applications and Information Systems 2014, WCCAIS, 2014, pp. 1–7.

[21] M.A. Alnatheer, A conceptual model to understand information security culture, Int. J. Soc. Sci. Humanit. 4 (2) (2014) 2–5.

[22] T. Dimkov, W. Pieters, P. Hartel, Laptop Theft: A Case Study on the Effectiveness of Security Mechanisms in Open Organizations, *CCS*, 2010, pp. 666–668.

[23] D.F. Sittig, H. Singh, Legal, ethical, and financial dilemmas in electronic health record adoption and use, Pediatrics 127 (4) (Apr. 2011) e1042–e1047.

[24] S. Alumaran, G. Bella, F. Chen, The role and impact of cultural dimensions on information systems security in Saudi Arabia national health service, Int. J. Comput. Appl. 112 (2) (2015) 21–28.

[25] B.B. Page, Exploring organizational culture for information security in healthcare organizations: a literature review, in: Portland International Conference on Management of Engineering and Technology, PICMET, 2017, p. 2017.

[26] S.R. Kessler, S. Pindek, G. Kleinman, S.A. Andel, P.E. Spector, Information security climate and the assessment of information security risk among healthcare employees, Health Inf. J. (2019) 1–13.

[27] F. Kamoun, M. Nicho, "Human and organizational factors of healthcare data breaches: the Swiss cheese model of data breach causation and prevention, Int. J. Healthc. Inf. Syst. Inf. 9 (1) (2014) 42–60.

[28] N.H. Hassan, Z. Ismail, Information security culture in healthcare informatics: a preliminary investigation, J. Theor. Appl. Inf. Technol. 88 (2) (2016) 202–209.

[29] M.A. Alnatheer, Information security culture critical success factors, in: 12th International Conference on Information Technology - New Generations Information, 2015, pp. 731–735.

[30] E. Sherif, S. Furnell, N. Clarke, An identification of variables influencing the establishment of information security culture, in: Human Aspects of Information Security, Privacy, and Trust, 9190, HAS, 2015, pp. 436–448. Lecture Notes in Computer Science, 2015.

[31] A. Da Veiga, N. Martins, Defining and identifying dominant information security cultures and subcultures, Comput. Secur. 70 (2017) 72–94.

[32] A. Nasir, R.A. Arshah, M.R.A. Hamid, S. Fahmy, An analysis on the dimensions of information security culture concept: a review, J. Inf. Secur. Appl. 44 (2019) 12–22.

[33] R. Mannion, H. Davies, Understanding organisational culture for healthcare, BMJ (November) (2018).

[34] A.B. Ruighaver, S.B. Maynard, S. Chang, "Organisational security culture: extending the end-user perspective, Comput. Secur. 26 (2007) 56–62.

[35] S. Furnell, A. Rajendran, Understanding the influences on information security behavior, Comput. Fraud Secur. (March) (2012) 12–15.

[36] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q), Comput. Secur. 42 (2014) 165–176.

[37] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, C. Jerram, A study of information security awareness in Australian government organisations, Inf. Manag. Comput. Secur. 22 (4) (2014).

[38] Badan Pusat Statistik Jawa Barat, Jumlah Penduduk Menurut Kabupaten/Kota (Jiwa), 2018-2020, 2018 [Online]. Available: https://jabar.bps.go.id/indicator/12/133/1/jumlah-penduduk-menurut-kabupaten-kota.html. (Accessed 25 November 2020).

[39] Badan Pusat Statistik, Jumlah Penduduk Hasil Proyeksi Menurut Provinsi Dan Jenis Kelamin (Ribu Jiwa), 2018-2020, 2018 [Online]. Available: https://bps.go.id/indicator/12/1886/1/jumlah-penduduk-hasil-proyeksi-menurut-provinsi-dan-jenis-kelamin.html. (Accessed 15 September 2019).

[40] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, Multivariate Data Analysis, 7/e, Pearson Prentice Hall, 2010.

[41] G.W. Corder, D.I. Foreman, Nonparametric Statistics for Non-statisticians: A Step-by-step Approach, 2009.

[42] M. Pett, Nonparametric Statistics for Health Care Research: Statistics for Small Samples and Unusual Distributions, Sage Publications, 2015.

[43] M. Alimohammadi, M. Yousefi, F.A. Mayvan, V. Taghavimanesh, H. Navai, A.A. Mohammadi, Dataset on the knowledge , attitude and practices of biomedical wastes management among Neyshabur hospital ' s healthcare personnel, Data Br. 17 (2018) 1015–1019.

[44] J.L. Fernández-alemán, A. Sánchez-henarejos, A. Toval, A.B. Sánchez-garcía, I. Hernández-hernández, L. Fernandez-luque, "Analysis of health professional security behaviors in a real clinical setting : an empirical study, Int. J. Med. Inf. 84 (2015) 454–467.

[45] B.P. Statistik, Labor Force Situation in Indonesia, 2018. August 2018.

[46] Ministry of Health Republic of Indonesia, Data Dan Informasi Profil Kesehatan Indonesia 2018, Jakarta, 2018.

[47] N. Humaidi, V. Balakrishnan, "Indirect effect of management support on users ' compliance behaviour towards information security policies, Heal. Inf. Manag. J. 47 (1) (2018) 17–27.

[48] Z.A. Soomro, M.H. Shah, J. Ahmed, "Information security management needs more holistic approach: a literature review, Int. J. Inf. Manag. 36 (2) (2016) 215–225.

[49] N. Van Deursen, W.J. Buchanan, A. Duff, Monitoring information security risks within health care, Comput. Secur. 37 (2013).