Unravelling the Ubiquitous Information Security Compliance Conundrum Among Practitioners In Private Healthcare Organisations Within Malaysia

Premylla Jeremiah[1], Ganthan Narayana Samy[2], Kannan Ponkoodalingam[3], Bharanidharan Shanmugam[4], Nurazean Maarop[5]

[1,2,5] Universiti Teknologi Malaysia, Malaysia
[3] INTI International University, Malaysia
[4] Charles Darwin University, Australia
Email: [1]pamjeremiah@gmail.com

ABSTRACT

Healthcare organisations worldwide are continuing to experience numerous information security incidents and breaches despite measures taken to safeguard themselves from such threats and attacks and this study investigates similar issues associated with the private healthcare organisations in Malaysia. A preliminary investigation was conducted from both healthcare and information security respondents through semi-structured interviews and the content analysis technique was used to derive common patterns found in them. The findings from the interviews show that often, the fault lies within the human aspect, i.e. the management and employees of the organisation itself. Some of the factors that have led to information security being compromised are the dearth of commitment from the management, having non-stringent security policies, behavioural issues, lack of security awareness and etc. The exposure from these risks will inevitably jeopardise the organisation's healthcare informational assets. Thus, to ensure the enforcement of information security policies and to mitigate the threats, proper compliance measures must be established throughout the healthcare organisation. The emerging recurring themes that were identified through the preliminary investigation will be used to guide and structure the mixed methods study in the next phase of the research

Keywords

Awareness, Behaviour, Compliance, Healthcare, Information Security, Threats

Introduction

A broad number of organisations from various industries today continue experiencing notorious information security attacks despite having intensified measures to overcome the dilemma (Safa et al., 2019). Critical industries such as healthcare are especially vulnerable to such attacks (Quick, 2016) and over the past decades, it is perturbing to discover that criminals often targeted healthcare information (Mamlin and Tierney, 2016) for malicious intentions and, seemingly there is no decline of information security breaches and incidents plaguing the healthcare industry throughout the world (Patil and Seshadri, 2014; He and Johnson, 2015). It is also disconcerting to know that despite the progress in healthcare security researches being studied and published (van Deursen et al., 2013), reported figures have further revealed that poor information security compliance, controls and compliance have caused immense errors and loss of millions of healthcare records (Fernandez-Aleman et al., 2015) which may eventually lead to unnecessary loss of lives. Thus the aim of this study is to investigate the causes that leads to information security breaches and incidents within the private healthcare industry in Malaysia. Moreover, the study will also address the various factors that are required to ensure how proper measures can be enforced and practiced to achieve good compliance in order to mitigate or reduce such incidents.

Literature Review

Information Security in Healthcare

In general, the healthcare industry mainly comprises of hospitals, clinics, nursing homes, pharmacies and other types of institutions that require healthcare information which involves diverse practices and procedures such as healthcare services, goods and facilities (Li et al., 2015), in addition to the latest medical technologies which have been developed for the usage of health-related information (Mamlin and Tierney, 2016). Therefore, the cornerstone for resolutions across all healthcare organisations infrastructure is through sound and reliable information (WHO, 2007), and this includes appropriate management and solicitation of health

information (Jensen et al., 2012) as it can enhance the value and security of healthcare (Mawilmada et al., 2012) as well as coordinate and deliver administrative efficiency in patient care (Kemkar and Dahikar , 2012). As such, information would be rather worthless if it is found to be inaccurate, untimely, not updated and difficult to obtain in order to meet the needs of various users within the healthcare sector. Indeed, in a critical industry such as healthcare, the preservation of consistent and timely information ensures that healthcare information users will not be denied from accessing reliable and functional information whenever needed (WHO, 2007; Koutsouris and Lazakidou, 2014).

Information Security Risks: Incidents and Vulnerabilities in Healthcare

Threats such as information breaches and incidents are a massive concern within healthcare organisations and they continue to escalate, despite the numerous solutions that have been developed to contain or eliminate them. Besides, various researchers in the past (van Deursen et al., 2013; Narayana Samy et al., 2010; Torabi et al., 2016) have presented an overview of risks and threats that can be damaging to the well-being of healthcare organisations as they can possibly affect the security of healthcare information assets. Apparently, most solutions developed through researches to mitigate such incidents were concentrated mainly on the technological dimension of the information systems (van Deursen et al., 2013) while other equally important elements such as human and organisational aspects were often overlooked. Another previous study by Appari and Johnson (2010) stated that security threats in healthcare organisation can generally be categorized into five different levels, in ascending order of sophistication as mentioned in Fernandez-Aleman et al., (2015), i.e. unintentional risks and exposure, prying by internal parties, information breach by internal parties, information breach with physical intrusion by external parties, and unlawful access on the network system. Hence, based on such classification, undoubtedly the majority of the threats and vulnerabilities are shown to have been indeed caused by the human factor as opposed to the technological element.

Thus, the issues faced by the healthcare organisations have not been solved in its entirety since there seemed to be a re-occurrence of past security breaches in which recent studies found that employee mistakes or unintentional actions continues to be the source of almost fifty percent of healthcare breaches (Poneman Institute,2016). Additionally, other literature from previous researches (van Deursen et al., 2013; Narayana Samy et al., 2010; Torabi et al., 2016) too have indicated that healthcare organisations must comprehend the various types of threats that can harm or damage their information assets, especially if they are made with malicious intention. In keeping with operational procedures and routine, most organisations usually monitor technical procedures and defences, while human error is often ignored or unheeded as a major cause of breaches (Fernandez-Aleman et al., 2015). However, healthcare organisations must uphold good information security practices and not overlook any form of threats or vulnerabilities from any possible root causes that can lead to irreparable damage to their information assets and may affect human lives.

According to a security study by SANS (Filkins, 2014), most healthcare practices are poorly protected due to the lack of information security compliance knowledge and other human behaviour issues among the employees and healthcare workers. In critical fields such as healthcare, all employees are expected to have some degree of awareness of the threats and vulnerabilities since they are dealing with highly valuable or critical information (Williams, 2008). Furthermore, breaches and vulnerabilities towards personal health records, billings, payments, intellectual property often occur since the healthcare organisations usually struggle when encountering new or different information security threats. The SANS study (Filkins, 2014) further mentioned that numerous medical, application systems and IT devices such as radiology imaging software, firewalls, printers, security application systems and etc. are easily targeted by criminals, thus making a way for malicious content to spread throughout the entire organisation due to inappropriate use of technology, as well as, ineffective safeguarding measures. In consequent, since the majority of healthcare staff are not provided with technical training in security matters, the lack of knowledge and awareness can create further unforeseen vulnerabilities (Williams, 2008. Hence, due to information

security misbehaviour, insufficient security training and an individual's level of awareness toward threats on information security could be low, significant information security breaches would continuously exist (Ogutcu et al., 2016).
These healthcare organisations have begun to realize the effects and havoc of the security breaches wrought upon them through such poor enforcement of information security, especially in confronting the challenges involved in securing their information systems (Behara et al., 2013) this issue is having effective information security awareness to create the necessary knowledge that would enable healthcare employees to be vigilant and responsible towards compliance of information security. As such, the implementation of information security awareness is deemed as a best practice and an important organisational factor to encourage and raise the level of compliance (Soomro et al, 2016; Page, 2017).

Preliminary Investigation with Qualitative Research Methods

A preliminary investigation study was carried out for the purpose of information gathering and to gauge the feedback and opinions from selected respondents. The qualitative research design was considered a suitable approach to collect data because it covers a gap in the healthcare environment as they provide researchers with a comprehensive outlook on work procedures, behaviours, actions, operations, perceptions, and culture in a way that quantitative research alone is unable to achieve. Besides, according to Creswell (2013), this research design can also be described as "an effective model that occurs in a natural setting that enables the researcher to develop a level of detail in being greatly involved in the actual experiences"

Data was collected by conducting semi-structured interviews and the rationale behind the selection of the semi-structured interview method was twofold: Firstly, to identify the main issues and challenges faced by the healthcare employees that leads towards information security misbehaviour and non-compliance among them. Additionally, the second reason is to gauge the feedback and opinion of the respondents regarding the essential need to investigate which measures are most effective in motivating, shaping and mitigating the employees' attitude and behaviour to create and raise the information security compliance levels within healthcare organisations. The feedback from the preliminary investigation will then be used to formulate the questions for the next phase of the research. This particular method was applied as it provided flexibility with the interview questions, thus allowing an unhindered, detailed line of questioning based on the interviewees' response.

Furthermore, the semi-structured interview was also deemed suitable for the research topic because it allowed the researcher to tailor the questions into the study's context and perspective (Creswell, 2013).

Participants' Background

The preliminary investigation involved interviewing well-experienced participants in various areas such as information security, healthcare systems and operations, healthcare management, information technology, and etc. The selection criteria for selecting the participants was to ensure that they have related working in their respective expert field for a minimum number of two years. In total, sixteen individuals from a spectrum of fields, designations and organisations were selected for the preliminary investigation study. Two participants were academicians from universities, one from Cyber Security Malaysia, one from a medical IT solutions company, and twelve from various private hospitals in Malaysia. The participants' job designations among others, were a medical academician, an information security academician, an information systems manager, medical doctors, a laboratory radiologist, a medical imaging technologist, nurses, Hospital IT administrators and etc. while their work experiences ranged from two to forty years as shown in Table 1 below. All identities remained anonymous in order to maintain the confidentiality of the participants' information during data analysis and in reporting the findings for the preliminary investigation study.

Table 1. Respondents' Distribution of Personal Details

No.	Specialization	Job Role	Work Experience
Respondent 1	Information and Cybersecurity	Security Consultant	14 years
Respondent 2	Networks and security	Security Academician	35 years
Respondent 3	Telemedicine	Medical Academician	40 years
Respondent 4	Medical Solutions Development	IT Consultant	12 years
Respondent 5	IT Security	IT Officer	4 years
Respondent 6	Information systems management	IT Administrator	7 years
Respondent 7	Information systems management	IT Manager	3 years
Respondent 8	General Practitioner	Medical Officer	7 years
Respondent 9	Patient care	Nurse	28 years
Respondent 10	Patient care	Nurse	2 years
Respondent 11	Cardiology	Consultant Cardiologist	35 years
Respondent 12	Preventive Medicine	Specialist	14 years
Respondent 13	Medical Imaging	Lab Radiologist	4 years
Respondent 14	Medical Imaging	Imaging Technologist	5 years
Respondent 15	Radiology	Specialist	17 years
Respondent 16	Gynaecology	Consultant Gynaecologist	32 years

Data Collection

The interview session for each participant were conducted between December 2018 and March 2019 as displayed in Table 1 above. Each session took between 50 minutes to 75 minutes to complete. Before the interviews were conducted, an interview guide was provided to all the participants. The purpose of the interview guide was to give them an overall idea about the preliminary investigation study, as well as, the interview procedure. Based on the interview guide, the main questions that were the focus in the interview are mentioned below:

- What are the information security problems, security incidents and vulnerabilities faced by private healthcare organisations that requires stricter enforcement of policies?
- What are the issues and challenges that hinders the private healthcare organisations from implementing and achieving compliance in information security?
- How to ensure compliance is achieved within the healthcare organisation?

Interview Analysis

The content analysis approach was selected as a research method as it can be extensively used to analyse qualitative descriptive data across a set of research questions (DSouza , 2017), into which the data analysis and interpretation can be further divided into several steps (Mertens, 2014) in order to identify, generate and organize initial codes into categories and subcategories before generating a report on the results through models, conceptual maps or categories and etc. (DSouza , 2017; Mertens, 2014; Miles et al., 2014; Vaismoradi, 2013). Since the purpose of this approach is to describe the phenomenon in context, therefore the content is analysed for distinct representations so that it can be expressed conceptually (Vaismoradi, 2013; Bengtsson, 2016; Queiros et al., 2017; Sutton and Austin, 2015). It is an approach that utilises systematic coding and categorizing which is generally used to produce the findings through examining textual information by determining the themes and patterns, their frequency, relationships, as well as the organisation and flow of communication in the interviews in order to draw the conclusion (Vaismoradi, 2013; Tajabadi et al., 2019; Kelley-Quon, 2018; Chang et al., 2020). Below are the steps that have been conducted in analysing and interpreting the interviews with the selected participants from the preliminary investigation:

Step 1: Data Preparation Phase

At this phase, all the data and field notes that were recorded and collected during the interview sessions are entered into NVivo 12 to assist with the transcribing and analysis process. As an example, an excerpt of the responses from the respondents that have been transcribed is shown below for the following interview question regarding the need of implementing stricter

enforcement of policies due to information security incidents in the workplace:

Question: What are the information security problems, security incidents and vulnerabilities faced by private healthcare organisations that requires the stricter enforcement of policies?

Respondent 1:

"The fact is that our systems and information can still get breached or exposed to some form of malicious attacks despite having firewall protection and other forms of intrusion detection software installed. Nowadays, all forms of malicious attacks can take place and if that happens, it will certainly create problems for the hospital. The employees are also facing possible threats especially when they are exposed to phishing emails, computer viruses, ransomware, hacking, pharming, denial of service, botnets, social engineering, unpatched security vulnerabilities and etc. Of course we have the backup data available, but we also have to be careful that the backup is updated regularly, is completely unharmed and not destroyed as well. Sometimes, the employees' negligence, errors or carelessness can cause compromise with the information security policies and this can lead to huge losses for the organisations should a security breach happen."

Respondent 2:

"There is an absence of information security compliance measures in some of the organisational procedures. There have been talks about it but it seems as though it has never been documented into an official security policy. There are also certain irrelevant information security policies that are considered rather outdated, as well as, there are those already existing policies that have unclear or ambiguous guidelines. The organisation needs to seriously look into the latest security issues such cybersecurity. I think there is a lack of awareness with such issues among our staff and this could lead to unwanted information security incidents".

Respondent 3:

"There are endless security problems and threats that we have to be very alert with. In fact, one of the possible threats that can harm our systems and patients' medical information could come from insiders' attacks. This can easily occur, especially when there are employees who may have spiteful or revengeful intentions, having grudges with the management or have bad intentions to cause harm to the workplace. They might steal highly classified, important information and sometimes, even damage or destroy this valuable information. These malicious acts disrupt our medical information systems, and sometimes damages the medical records and other related information such as financial accounts, payment, credit card numbers, insurances and etc. At times, the organisations also create tempting targets for security incidents or threats to happen such as data breach, misconfiguration, insecure interfaces, flaws in the firewall, account hijacking, Trojans and etc. If any security incidents or breaches occur, then this means that the healthcare organisations staff would be responsible for their own negligence. Also, they were not maintaining their security technology securely and effectively with the latest security updates and patches."

Question: What are the issues and challenges that hinders the private healthcare organisations from implementing and achieving compliance in information security?

Respondent 1:

"Actually, most of the employees are not aware of many issues that are linked to information security. They lack the knowledge required with regards to being responsible and compliant. There's a lack of education and training as well, so employees make mistakes with information security unintentionally because they are completely ignorant. Sometimes, they find it difficult to understand the user guides on information security policies as they may be too technical or complex. The older staff certainly have found it challenging to adapt themselves in using technology and to make things harder, almost everything is computerised or in digital format, so they time to learn. Acceptance is not easy for them because they are used to doing things manually. Also, they find it very cumbersome to remember passwords or secret codes for every machine or piece of equipment. Some of them have complained that they write down their passwords on their desks because they might forget, especially if they are required to change the passwords every three or four months.

So, in fact, many of them are experiencing information security fatigue because they feel overworked when dealing with security and eventually feel stressed and tired. It's affecting their moods and behaviours and sometimes, they become reluctant when they asked to enforce information security."

Respondent 2:

"There is very poor information security culture in the most healthcare organisations and this would actually reflect among the employees in the workplace environment. Usually, if there is good information security culture in place, then, usually it will influence the workers because they can see and realise that their bosses, peers and all other colleagues within the workplace are following the culture well, with hardly any compromise or slack in enforcing information security compliance. Most importantly, the implementation of good security culture can have an effect on the behaviour of employees and it can also be used to guide or motivate employees to follow the proper implementation of information security policies. The organisation or, should I say, the management needs to ensure that the level of awareness and acceptance of compliance must always remain high among the employees. If the level of awareness and acceptance of compliance is low, we would be encountering difficulties in ensuring the staff to comply with the compliance policies. The management themselves needs to be proactive in their approach towards adopting good information security compliance policies and achieving compliance properly. In other words, if the management themselves lack the commitment, then how would you expect to change the work culture around here? So, both employees and the management must support each other in providing a strong information security culture so that good compliance levels will always be achieved and retained."

Respondent 3:

"Sometimes the issues could be coming from unintentional errors or threats such as carelessness or negligence by our own employees when handling the information. Besides this, staff can also experience information security fatigue and they tend to compromise with the information security policies because they are overworked and burnout. Everyone should be responsible in practicing good compliance and it's not easy because we are dealing with humans. In my experience, some people are just about impossible to manage or handle. They have mood swings and attitude problems such as being egoistic, lazy, old die-hard habits that are difficult to change, carelessness, irresponsible and the list goes on. At the end of the day, I will just say that generally, it's their attitude, more than anything else, which usually is the reason for information security problems to occur and these problems are the ones that causes the organisation to fail in achieving compliance."

Question: How to ensure compliance is achieved within the healthcare organisation?

Respondent 1:

"To ensure that the employees would comply well at all times, there must be must some form of motivation or encouragement from the management. Encouragement can come in many forms such as getting appreciation notes from the management, rewards or incentives for employees who adhere strictly to compliance policies, good bonuses or salary increments, and even goodie hampers and etc. The employees would certainly be pleased with these acknowledgements from their employer and will certainly strive to maintain their performance in complying with the organisation's security policies. And as for employees who have acted irresponsibly or did not care to practice good compliance behaviour, they should be given penalties or sanctions, in order for them not to repeat these offences. By giving them penalties, they would then understand and become aware that complying with information security policies is compulsory and an important priority for the organisation."

Respondent 2:

"I always believe that education is the key to creating security awareness. Employees can be exposed to different methods of learning and this can help to instil knowledge that is required to manage information security in healthcare. Trainings and seminars can also be conducted periodically, so that updates and practical hands-on applications on information security can be given to all employees. Besides providing information security education and training to the employees, the management should also be

actively involved in promoting a strong information security culture in the everyday working environment of the organisation. A strong information security culture is important because it guides how things are done in organisation in regards to information security. Employees are more likely to think and act in a security-conscious manner because it influences the employees' security behaviour. Information security culture also helps to cultivate awareness among employees and with this knowledge, they will learn to protect the information assets and help mitigate against a range of threats that could cause physical, reputational or financial damage to the organisation."

Respondent 3:

"The organisation can try to implement the usage of triggering software like games or videos which has interactive functions that can influence or persuade the employees. I have seen such applications in my wife's company and I find it very interesting. We can learn from viewing and using these kinds of software. If the content is interesting and good, it would be worth setting aside some budget and spending the money to purchase such software. So if the management decides to purchase them, it only shows that the management is very committed in wanting to improve the rate of good compliance behaviour among the employees. With today's situation where there are so many information security problems that are happening almost every day, then having a management that is committed is extremely necessary especially when they can provide substantial yearly budgets for making purchases meant for information technology that would benefit the organisation. I also believe that the management must monitor all the employees and their usage of information technology systems and information thoroughly, especially to help reduce security breaches caused by insiders. Monitoring is important because it helps to identify users who are non-compliant and stern actions need to be taken on these users to ensure their non-compliance actions or misbehaviour will not be repeated. Since employees' non-compliance actions and behaviour can be advised and corrected with monitoring, it would significantly reduce information security misbehaviour. They would also tend to be more responsible in their duties and try their best to avoid making mistakes or being careless."

Table 2. Exploration of Themes and Codes

Respondent 1	Exposure to malicious attacks Having firewall protection and other forms of intrusion detection software installed Information security attacks will create problems Ensure backup is updated and safe Unintentional errors or threats Employees' carelessness or negligence Experiencing information security fatigue Compromising with the information security policies
Respondent 2	Absence of information security compliance measures No proper information security documentation for certain procedures Irrelevant information security policies Rather outdated policies Unclear or ambiguous guidelines in existing policies Look into latest information security issues Lack of awareness
Respondent 3	Low level of awareness and acceptance in compliance Proactive and committed management Everybody should be responsible Some people are just about impossible to manage or handle Mood swings, attitude problems such being egoistic, lazy, old die-hard habits that are difficult to change, carelessness, irresponsible, arrogant and the list goes on Poor attitude that might cause information security breaches

Step 2: Data Exploration

In the exploration phase, the data from the transcribed responses are read through to translate their meaning as well as to look for codes and themes. Important and relevant parts of the text are highlighted and emphasized. Table 2 below

shows an excerpt of several themes and codes that were derived from the participants' responses in Step 1.

Step 3: Data Reduction Phase

The reduction process includes identifying and perceiving common patterns in the data. Furthermore, this phase helps to create codes that describes the data patterns and assigning the codes which will then serve to reduce the data from an overwhelming pile of transcripts and notes into a meaningful depiction of the problem being studied in the research. The data reduction process displayed in Table 3 below provides common patterns in the data that was transcribed earlier in Steps 1 and 2. The data was derived from the responses of all the sixteen participants whose answers were based on the main questions posed in the interview. From the data reduction phase, it became apparent that all sixteen participants provided almost similar responses whereby most of the current information security problems, vulnerabilities and issues identified within the private healthcare sector in Malaysia are stemmed from the human element. Thus, the elicitation of this information would eventually lead to the initial findings depicted in Table 4 in which a further breakdown of the pattern of data perceived during the reduction phase is construed and observed. Furthermore, in Table, 4 all the vulnerabilities, issues and themes pertaining to information security in healthcare organisation' s that were derived from the preliminary investigation study have been further segregated and categorized accordingly under the Human, Organisational and Technological (HOT) elements.

Table 3. Data Reduction Process

Compliance	Operations security	Information security of mobile devices	Physical and environmental security
Risk and threat environment	Awareness	Information security of IT-medical devices	Motivation
Irrelevant security policies	Education and training	Attitude/ Behaviour	Business continuity
Outdated enforcement of policies	Communication security	Information classification	Ethical conduct
Absence of IS compliance measures in organisational procedures	Lack of management commitment	Information security for non-IT medical and non-medical devices	System acquisition, development and maintenance
Information storage media	Supplier relationships	Cryptography controls	Roles and responsibilities
Obligation to comply	Non-stringent policies	Information security fatigue	Safeguards and defences
Audit	Work culture	Unclear policy guidelines	Compromise
Malicious Intentions	Trust	Habits	Expectations
Convenience	Logging and Monitoring	Emotions	Non-malicious causes
Ego/ Superiority/ Pride	Irrelevant enforcement of policies	Social Norms	Negligence
Unintentional errors/threats	Operational Procedures	Backup	Incentives/ Rewards

Results

Initial Findings

Several initial findings and results have been derived from the preliminary investigation study and the respondents' responses and feedback were then sought to ascertain if the private healthcare organisations in Malaysia face information security threats and incidents that will cause information security problems, which then could lead to damaging effects. Additionally, the findings on issues and challenges that hinders the private healthcare organisations from implementing and achieving compliance in information security were also revealed. Finally, the respondents also disclosed several important measures in which they perceive could raise and achieve the level of good information security compliance within the private healthcare industry.

Derivation of Information Security Compliance Issues

The feedback garnered from the respondents provided insights and opinions on the current issues and challenges of enforcing information security compliance in the respective healthcare organisations in Malaysia. Following the feedback that was received, any information security issues that emerged from the interviews related to the threats, breaches, vulnerabilities and any security-related incident that could compromise healthcare organisations were also identified. The issues were based from the respondents' feedback as identified in Table 4 below, demonstrates a real need for stricter enforcement of compliance in healthcare. Despite the compulsory implementation of an Information Security Management Systems based on ISO 27001 Standards in all of the private Malaysian healthcare organisations since 2013 (ISO, 2016), there still exists an underlying issue with the actual enforcement of information security compliance. Therefore, this pertinent issue with information security compliance within a highly critical industry establishes an existing research gap that requires immediate attention so that the problem can be mitigated further. Furthermore, the issues that were identified during the preliminary investigation are inexorably linked to the Human, Organisational and Technological (HOT) elements and as emphasised in Table 4, most of the threats or breaches were caused by humans rather than technology. According to the respondents, most of the factors indicated the Human or People dimension is undoubtedly, the 'weakest link' or main impediment that have caused and, ultimately resulted in the lack of proper enforcement in complying with standards and polices in the workplace. This feedback supports the findings from earlier researches [23] that revealed most healthcare employees, regardless of the job category and level, have behavioural problems which are perceived as the main source for information security breaches. Moreover, evidence from both the preliminary investigation and past studies have clearly shown that behavioural issues is indeed one of the main reasons for failing in meeting information security requirements for compliance. Likewise, the findings from the preliminary investigation have shown that there were many factors that inevitably induced behavioural problems among healthcare employees, namely they tend to be lacking in many different aspects of information security misbehaviour such as information security culture, work ethics, awareness, information security fatigue, attitude, education, training, carelessness, ignorance and etc. as indicated in Table 4. Based on the issues that are presented in Table 4, this research has further identified critical and stringent measures that are perceived to help enforce and strengthen compliance among the users in the healthcare organisations. Thus, in order to cultivate and increase a more positive stance in the behaviour of healthcare employees towards the proper implementation of security compliance and policies, this research proposes several underpinning measures to oversee that the standards and controls for information security are adhered accordingly with a more stringent enforcement within the private healthcare organisations in Malaysia. As a result, based on the summary of the literature and research findings, several important elements such as Awareness, Security Education and Training, Organisational Security Culture, Rewards and Sanctions, Persuasive Technology, Management Support, and Monitoring, have been identified and proposed as critical compliance measures (Herath and Rao, 2009; Kessler et al., 2020) that are required in order to achieve compliance which would eventually lead to attaining value delivery for the organisation. These critical compliance measures and their corresponding attributes will

be further examined and studied among the healthcare, IT and security personnel to examine its validity in ensuring success in meeting compliancy of healthcare organisations in the next phase of the research.

Table 4. Feedback derived from the Preliminary Investigation

Identification of Information Security Compliance Issues in Malaysian Private Healthcare Organisations (HOT Elements)		
Human (H)	**Organisation (O)**	**Technology (T)**
Attitude/ Behaviour	Lack of management commitment	Information security of mobile devices
Awareness	Risk and threat environment	Information security of IT-medical devices
Education and training	Irrelevant security policies	Information storage media
Ethical conduct	Non-stringent policies	Information classification
Compliance	Absence of IS compliance measures in organisational procedures	Information security for non-IT medical and non-medical devices
Information security fatigue	Unclear policy guidelines	Physical and environmental security
Negligence	Outdated enforcement of policies	Cryptography controls
Obligation to comply	Formal disciplinary process	Safeguards and defences
Malicious Intentions	Operational Procedures	Operations security
Habits	Information security incident management	Logging and Monitoring
Non-malicious causes	Audit	Communication security
Unintentional errors/threats	Risk Assessment	System acquisition, development and maintenance
Ego/ Superiority/ Pride	Roles and responsibilities	Access control
Compromise	Business continuity	Backup
Convenience	Financial costs	
Emotions	Inventory of assets	
Incentives/ Rewards	Supplier relationships	
Work culture		
Motivation		
Expectations		
Trust		
Social Norms		

Discussion

From the findings of the preliminary investigation, all the participants have unanimously acknowledged that currently, there are still numerous information security incidents and issues that have continued to create on-going challenges in achieving compliance within the healthcare industry. The findings also show that it is also evident that the initiatives undertaken by the private healthcare organisations towards the compliance of information security management are currently below satisfactory levels. Thus, in order to establish better compliance levels, it was perceived that it is highly imperative that stricter measures of enforcement be established and implemented by the private healthcare organisations. Past literature and findings derived from the preliminary investigation have indicated that a significantly vital dimension such as

Security Awareness and other equally important antecedents which include Organisational Security Culture, Education and Training, Rewards and Sanctions, Persuasive Technology, Management Support, and Monitoring will be discussed further as these have been perceived to raise the levels of compliance of healthcare employees in each of their respective organisations. Figure 1 below depicts the conceptual perspective for information security awareness and all the corresponding attributes that is prevalent in fortifying information security compliance.

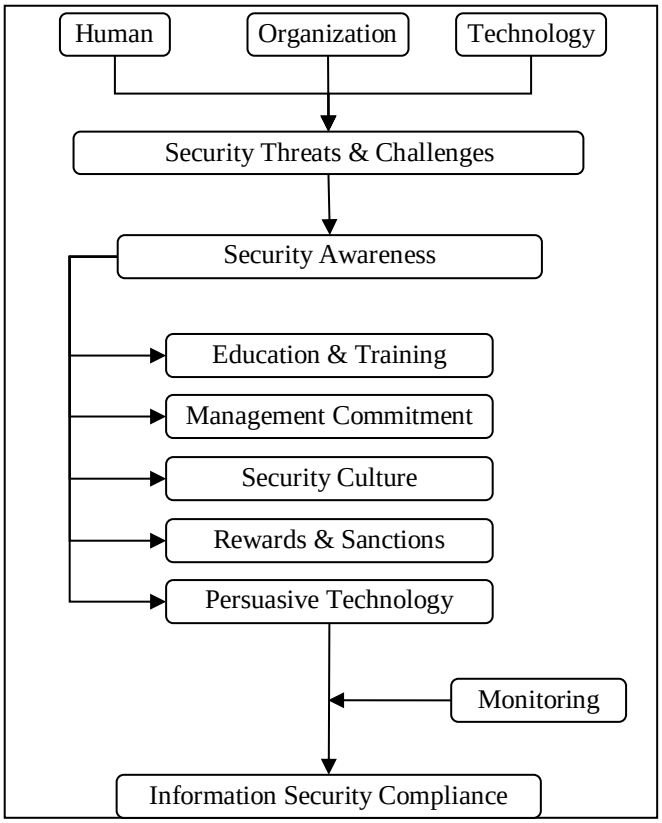

Figure 1. Conceptual perspective for information security awareness

Information Security Awareness

One of the most effective and fundamental measures that can be used to cultivate and increase compliance is to ensure that security awareness is developed and disseminated throughout the healthcare organisation to all levels of employees. In order to promote good information security practices for achieving compliance, information security awareness needs to be inculcated to shape the attitude and behaviour of employees in the workplace [27]. Through establishing and enabling security awareness campaigns, healthcare employees would be able to increase their security knowledge and improve on their personal efficacy. Most of the respondents have also agreed that the lack of security awareness has caused many information and data breaches to transpire because of human error, carelessness or ignorance. Below are several excerpts from the participants' responses:

".....Awareness is severely lacking and we really need to take drastic actions like championing the cause for awareness continuously or engaging the entire organisation by conducting various activities such as having an awareness week or awareness month on information security just to instil that sense of awareness with our employees."

"……Because of the lack of security awareness, many employees are simply ignorant about how critical information security is. We need to embark on awareness campaigns every now and then."

Additionally, there are numerous measures that ought to be included for ensuring the development of information security awareness would be successful in achieving good compliance levels through engaging with exemplary compliance behaviour. The measures were derived from literature review, as well as, the findings from the preliminary investigation and would be discussed in further detail below:

Security Education and Training

Findings from the interview further revealed that heavy workload and extreme work pressure had also contributed to the non-compliance towards information security policies. Due to this sense of fatigue, they even refused to comply with the most basic information security policies such as changing passwords, logging off the computer systems, creating backups, leaving systems unattended and etc., thus exposing the environment to threats and breaches. Therefore, in order to overcome these issues, key findings from past studies [30] have proposed various methods on how Security Education and Training (SET) could be implemented as a compulsory reinforcement among employees, in order to create better awareness on the importance of information security, as well as, motivate and engage their behaviour for achieving compliance.

Therefore, as part of the SET programme or campaigns, we would like to suggest that live practical lessons with a 'surprise' element, especially on social engineering, phishing spamming and etc. be occasionally given to all ranks and categories of healthcare employees in order to test their actual levels or point of awareness as well as their actual behaviour towards information security compliance. As such, the 'surprise' element that could be incorporated in these practical sessions would be keeping the live test's date and time undisclosed, otherwise it will produce results that may not be accurate and unrealistic.

Another aspect of SET that was proposed by many respondents was the emphasis on certain high-risk issues that often times surfaces such as in endpoint security, especially since it is the norms to bring your own device (BOYD) which may include notebooks, smartphones, tablets and etc. to the workplace. These devices are particularly vulnerable because humans are often the weakest link and will blindly click on a link in an email, connect a laptop to an unfamiliar network, carelessly leave a smartphone lying around, or leaving computer monitors unattended for long periods of time without screen savers or passwords and etc. All of these innocent or unintentional mistakes can lead to a loss or compromise of sensitive information for the healthcare organisation, and therefore, could lead to terrible repercussions which might require a public acknowledgement of breach that would further taint the organisation's good name and image.

In corresponding to their answers, we would like to further recommend that the top management of these healthcare organisations seriously consider identifying the most suitable means of delivering SET from a wide range of resources that is easily made available i.e. workshops, seminars, campaigns, newsletters, e-mail reminders, screen savers, pamphlets, multimedia/game tutorials, awareness quizzes and etc. Furthermore, the organisations should identify the different category of users and learners within the healthcare facility i.e. information systems personnel and end-users (medical personnel) so that the SET package could be customized accordingly to better suit the needs and requirements of each group.

Organisational Security Culture

Organisational security culture is deemed indispensable towards the development of information security awareness in the workplace. In the perspective of information security, organisational security culture can be recognised as an influential dimension of security awareness when the employees assimilate the information security policies and integrate with the security practices accordingly in their everyday activities. Evidently, security-aware culture is nurtured and developed when the employees embrace information security as a regular aspect with their working environment. The establishment of an organisational security culture can have an impact on the employee' security behaviour because essentially, the environment can influence their working lifestyle and everyone around them. New employees can learn to adapt to such working climate and with having every person within the workforce to comply with the security policies, the organisation will eventually have an advantage because they would have earned the capability to significantly reduce the threats or risks to information assets.

Rewards and Sanctions

Provision of incentives and stringent enforcement of appropriate sanctions were also proposed by several of the respondents as a means of shaping, engaging and motivating the healthcare employees' attitude and behaviour to practice compliance. As an essential measure that can be implemented to increase information security awareness, the rewards-based measures would certainly increase the motivation levels while the sanctions-based measures would instil a sense of fear and could determine the success rate of compliance (Dsouza, 2017). Past studies have reported that computer misuse was considerably reduced with sanctions (Dsouza, 2017; Sutton and Austin, 2015; Tajabadi et al., 2019) and employee compliance with information security policies was increased (Dsouza, 2017; Kelley-Quon , 2018).

Management Support

Additionally, having a responsible management which is committed to the information security compliance cause is also another crucial supporting aspect in developing information security awareness, as well as, motivating and

persuading the healthcare employees to engage themselves with good workplace ethics, attitude and behaviour. Several respondents claimed that the upper management almost stays "invisible" when it comes to handling sensitive issues such as information security breaches and threats. Without proper commitment, it will be very difficult to engage or persuade the workforce to adopt an information security workplace culture as they would tend to think that these information security issues are not the crux of the matter, based on their observation of the non-committal attitude of the management.

Persuasive Technology

The development of persuasive technologies are intended to allow for both behavioural and attitude changes with the aid of interactive computing. The implementation of persuasive technologies can effectively influence or change human behaviour through the elements of motivation, ability and trigger, but not with coercion, deceit or manipulation. Today, many systems such as games and mobile applications have developed persuasive technologies to enable or motivate behavioural changes. For healthcare organisations, the concepts of perceived persuasiveness must be designed into the systems to stimulate and motivate awareness of information security. Besides stimulation, instructions or recommendations must also be developed into the systems so that users can receive advice on information security. Moreover, persuasive technologies have the high potential to enhance the security of working environment and practices, to create long-term impact to increase or improve sustainability of the healthcare employees' security awareness and behaviour.

Monitoring

Monitoring is also an essential component that needs to be incorporated and conducted periodically to ensure that the security policies and procedures are not compromised among the employees of any department within the healthcare organisation. It is a significant factor in the development of information security awareness as it is a core responsibility of the management of the healthcare organisation, to ensure enforcement of the security policies and procedures from every individual and department within the organisation is monitored, measured and evaluated accordingly. The healthcare organisation will also need to persistently monitor and measure the degree or extent of compliance, especially among their workforce at all levels of operational procedures. Through rigorous monitoring and measuring taken periodically from time to time, they would be able to evaluate the level of success or failure in achieving compliance. Successful results must be strictly maintained while further action ought to be taken in cases where compliance has yet to meet its satisfactory mark.

Hence, the proposed compliance measures and dimensions (Herath and Rao, 2009; Kessler et al., 2020) also play a critical role in ensuring that compliance can be practiced and complied without any impediments. Altogether, these factors would eventually lead the healthcare organisation to attain successful compliance which in turn, will generate the desired value delivery. The value delivery is anticipated to bring forth perceived benefits such as protecting the assets and deliver business value to stakeholders, ensuring and maintaining accountability, effectively managing security risks, raising awareness at both the management level and entire organisation, have stronger measures of enforcement, as well as, creating defences to safeguard against the threats, incidents and vulnerabilities in order to always ensure a high level of compliance in healthcare information security compliance.

Conclusion

This paper presents the initial findings of information security incidents and threats that are prevalent today, information security compliance enforcement challenges in private healthcare organisations, as well as, measures that can be implemented to raise the levels of compliance among the healthcare employees based on the preliminary investigation interviews that were carried out. The insights and feedback garnered from the preliminary investigation were used to propose measures to mitigate or reduce security threats and breaches which are perceived to yielding in value delivery such as reputation, branding and trust for the organisation. Furthermore, it would significantly create long-term awareness and compliance among the healthcare employees and these aspects would

also enhance the security of the patients' vital information that is critical to the company. More in-depth research and further examination will be conducted on the security literature in the future works of this study. Furthermore, an empirical research would also be carried out whereby a research model will all these potential dimensions and variables will be developed and analysed statistically to investigate the outcomes and significances of enforcing these appropriate measures for creating information security compliance among healthcare employees.

References

[1] Appari, A. and Johnson, M. E., (2010). "Information security and privacy in healthcare: current state of research", International Journal of Internet and Enterprise Management, 6(4), 279–314.

[2] Behara, R., Huang, D. and Goo, J., (2013). "The emerging healthcare service platform", Kendall Hunt Publishing Company, Dubuque, Iowa, USA, 153-169.

[3] Bengtsson, M., (2016), How to plan and perform a qualitative study using content analysis, Nursing Plus Open, Volume 2, Pages 8-14,

[4] Chang S-I., Chang L-M., Liao J-C., (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach, Information & Management, Volume 57, Issue 6.

[5] Creswell, J. W., (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, (Fourth Edition), SAGE Publications, Inc.

[6] DSouza, M.J. (2017), "The Practice of Qualitative Research", Qualitative Research in Organizations and Management, Vol. 12 No. 3, pp. 247-248.

[7] Fernandez-Aleman, J. L., Sanchez-Henarejos, A., Toval, A., Sanchez-Garcia, A. B., Hernandez- Hernandez I., Fernandez-Luquec, L., (2015). "Analysis of health professional security behaviors in a real clinical setting: An empirical study", International Journal of Medical Informatics, 84, 454–467.

[8] Filkins, B. (2014). "Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon", A SANS Analyst whitepaper, The SANS Institute InfoSec Reading Room. Available from https://www.sans.org/reading-room/whitepapers/ analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

[9] He, Y. and Johnson, C. W., (2015). "Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template". International Journal of Medical Informatics, 84(11): 941-949.

[10] Herath, T. and Rao, H. R., (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", Decision Support Systems.

[11] International Organization for Standardization, (2016), ISO/IEC 27799:2016, "Health informatics – information security management in health using ISO/IEC 27002", Available from <http://www.iso.org/iso/home.htm/>

[12] Jensen, P. B., Jensen, L. J., and Brunak, S., (2012). "Mining electronic health records: towards better research applications and clinical care", Nat Rev Genet 2; 13(6):395-405.

[13] Kelley-Quon, L. I., (2018). Surveys: Merging qualitative and quantitative research methods, Seminars in Pediatric Surgery, Volume 27, Issue 6, Pages 361-366.

[14] Kemkar, O.S., and Dahikar, P. (2012). Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Cost Using Latest Advancements in ICT for Better Interactive Healthcare Learning.

[15] Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A. and Spector, P.E., (2020), Information security climate and the assessment of information security risk among healthcare employees, Health Informatics Journal, Vol. 26(1) 461–473.

[16] Koutsouris, D-D., and Lazakidou, A. A., (2014), Concepts and trends in Healthcare Information Systems 10.1007/978-3-319-06844-2.

[17] Li, S., Feng, B., Chen, M. and Bell, R. A., (2015). "Physician review websites: effects of the proportion and position of negative reviews on readers' willingness to choose

the doctor", Journal of Health Communication: International Perspectives, 20(4), 453–461.

[18] Mamlin, B. W. and Tierney, W. M., (2016). "The promise of information and communication technology in healthcare: extracting value from the chaos", The American Journal Of The Medical Sciences,Volume 351 Number 1

[19] Mawilmada, P. K., Smith, S. E. and Sahama, T. R., (2012). "Investigation of decision making issues in the use of current clinical information systems", in Maeder, A. J. and Martin-Sanchez, F. J (Eds.) Proceedings of Health Informatics: Building a healthcare future through trusted information - Selected papers from the 20th Australian National Health Informatics Conference (HIC 2012), ISO Press, Sydney Convention & Exhibition Centre, Sydney, NSW, pp. 136-143.

[20] Mertens, D. M., (2014). "Ethical Use of Qualitative Data and Findings", in Flick, Uwe (ed.), The Sage Handbook of Qualitative Data Analysis, London: Sage, pp. 510-523.

[21] Miles, M. B., Huberman, A. M., and Saldana, J., (2014). Qualitative Data Analysis: A Methods Sourcebook. Thousand Oaks: Sage, ch. 2 (pp.17-54) and 11 (pp. 275-322).

[22] Narayana Samy, G., Ahmad, R., and Ismail, Z., (2010). "Security threats categories in Healthcare Information Systems", Health Informatics Journal 16 (3), 201-209.

[23] Ogutcu, G., Testik, O. M. and Chouseinoglou, O., (2016). "Analysis of personal information security behavior and awareness", Computers and Security, 56, 83–93

[24] Page, B. B. (2017). "Exploring Organizational Culture for Information Security in Healthcare Organizations: A Literature Review," Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, 2017, pp. 1-8, doi: 10.23919/PICMET.2017.8125471.

[25] Patil, H. K. and Seshadri R., (2014). "Big data security and privacy issues in healthcare", Published in Big Data (BigData Congress), IEEE International Congress, 25 September

[26] Queiros, A., Faria, D., and Almeida F., (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods, European Journal of Education Studies - Volume 3, Issue 9

[27] Quick, B. E., (2016). "Breach control: Best practices in health care application security, The SANS Institute Infosec Reading Room", Available from https://www.sans.org/reading-room/ whitepapers/ hipaa/ breach - control – practices – health - care-application-security-36765B.E.

[28] Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., Sookhak, M., (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations, Future Generation Computer Systems, Volume 97, Pages 587-597.

[29] Soomro, Z. A., Shah, M. H and Ahmed, J., (2016). "Information security management needs more holistic approach: A literature review", International Journal of Information Management, 36, 215–225.

[30] Sutton, J., and Austin, Z. (2015). Qualitative Research: Data Collection, Analysis, and Management. The Canadian Journal of Hospital Pharmacy, 68(3), 226–231

[31] Tajabadi, A., Ahmadi, F., Asl, A. S. and Vaismoradi, M. (2019). Unsafe nursing documentation: A qualitative content analysis. Nursing Ethics. doi: 10.1177/0969733019871682

[32] The Poneman Institute, (2016). "The Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data".

[33] Torabi, S. A., Giahi, R., and Sahebjamnia, N., (2016). "An enhanced risk assessment framework for business continuity management systems", Safety Science, Vol 89. Pp 201 – 218.

[34] Vaismoradi M, Turunen H, Bondas T. (2013). Content analysis and thematic analysis: implications for conducting a qualitative descriptive study. Nurse Health Sci. Sept; 15(3):398-405.

[35] van Deursen, N., Buchanan, W. J., and Duff, A. (2013). "Monitoring information security risks within health care", Computers & Security, doi: 10.1016/j.cose.2013.04.005.

[36] Williams, P. A. H., (2008). "In a 'trusting'

environment, everyone is responsible for information security", Inf. Secur. Tech. Rep.13 (4), 207–215.
[37] World Health Organisation (WHO), (2007). “Everybody's business: Strengthening health systems to improve health outcomes: WHO's Framework for action”, Geneva, WHO, 1-56.