Potential Measures to Enhance Information Security Compliance in the Healthcare Internet of Things

Premylla Jeremiah[1](✉), Ganthan Narayana Samy[1],
Bharanidharan Shanmugam[2], Kannan Ponkoodalingam[3],
and Sundresan Perumal[4]

[1] Advanced Informatics Department,
Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
pam_jeremiah@yahoo.com, ganthan.kl@utm.my
[2] School of Engineering and Information Technology,
Charles Darwin University, Casuarina, Australia
Bharanidharan.Shanmugam@cdu.edu.au
[3] Faculty of Information Technology and Science, INTI International University,
Nilai, Malaysia
pon.kannan@newinti.edu.my
[4] Faculty of Science and Technology, Universiti Sains Islam Malaysia,
Nilai, Malaysia
sundresan.p@usim.edu.my

Abstract. Healthcare organisations are particularly vulnerable to information security threats and breaches due to the highly confidential nature of their patients' medical information. Now, with the emergence of the Internet of Things (IoT) in healthcare that can vary from diagnostic devices to medical wearables, the industry has indeed become more vulnerable to malicious exploitation. One of the reasons that malicious attacks continue to occur at an alarming rate is due to the poor compliance of information security policies. This study investigates the issues that are associated with the causes for poor compliance within the private healthcare organisations in Malaysia. Data was collected through interviews from various healthcare respondents and findings have revealed that often, poor security compliance is mainly caused by behaviour issues and the severe lack of security awareness which requires immediate attention and mitigation. Potential measures to cultivate information security awareness and to safeguard the IoT-based medical devices are proposed to achieve compliance.

Keywords: Awareness · Behaviour · Healthcare · Internet of Things
Information security compliance

F. Saeed et al. (Eds.): IRICT 2018, AISC 843, pp. 726–735, 2019.
https://doi.org/10.1007/978-3-319-99007-1_67

1 Introduction

We live in a digitally connected world, in an age where the speed of technology is advancing rapidly and in which our environment and communities are seamlessly interwoven through the implementation and usage of the latest technologies and facilities. One such emerging cutting-edge technology that has penetrated its way globally is the Internet of Things (IoT) technology which are smart-enabled embedded computing devices [1] and thus, has been hailed as the revolutionary intelligent technology that will offer much potential for business ventures, innovate the way industries operate and even causing our lifestyles to be changed positively. Inevitably, one of the most critical mission industries that has prominently implemented and reaped benefits from IoT is the healthcare industry. It may still be in its infancy stages in many healthcare organisations worldwide [2], but it is indeed a promising trend and is expected to redefine medical technology and healthcare, profoundly impacting the industry in the near future.

However, with such acceleration in the IoT-based healthcare technology and applications, the ensuing risks and vulnerabilities specifically in the area of information security also emerges and could prove to be a socio-technological and organisational challenge [3, 4] if not mitigated during its initial stages. The lax of security in IoT technology for the growing number of healthcare and medical devices could involve cyber risks [5] that may cause both virtual as well as physical harm [4] i.e. increased risk of bodily harm from a patient's breached clinical records or hacked medical devices whose information is now exposed to the criminals who can use it for unscrupulous reasons. In order to mitigate or avoid such vulnerabilities or risks from happening all together, several information security measures such as education, training, awareness campaigns, and technological safeguards [6, 7] must be introduced, enforced and adhered to, in ensuring that the privacy, confidentiality and integrity of the patients' healthcare information remains secured and not jeopardized.

Thus the aim of this paper is to investigate the causes that leads to IoT information security non-compliance within the healthcare industry and the information security awareness measures that can be recommended and enforced to help raise and achieve the levels of security compliance in order to mitigate or reduce the IoT-based vulnerabilities. This paper is organized into seven sections. The next section describes the literature review related to this research. Section 3 discusses the research problem while Sect. 4 explains the research methodology that is applied in this research. Section 5 presents the findings of the studies, Sect. 6 presents the discussion, and followed by a conclusion in Sect. 7.

2 Internet of Things (IoT)

Originally defined during the mid-1990s, the term 'Internet of Things' was used to describe the networked radio-frequency identification (RFID) infrastructures and sensor technologies [8]. Today, the usage of the IoT is wide and diversified, extending towards more and more domains and fields which are totally transformed by the capabilities, efficiency and effectiveness that IoT technology brings [9]. Some of the more prominent domains that have been dynamically implementing IoT-enabled applications would include transportation, automotive, healthcare, manufacturing, agriculture, smart cities and homes, and etc. Powered by the latest enabling technologies such as smart sensors and Near Field Communication (NFC) as well as the interplay with cloud computing, big data analytics and fog computing, the IoT is anticipated to aggressively fuel the transformation of many emerging intelligent devices, applications and technological innovations to match user requirements, compatibility, as well as market demands in terms of effectiveness and efficiency, for any moment and any place [10] in the imminent future.

3 IoT in Healthcare

Among the various domains that have deployed IoT technology and applications, medical and healthcare has become one of the most widespread and well-represented within the last few years [3] in which many highly significant changes have been brought about. These timely interventions in healthcare have not only brought a sharp surge in improved patient clinical care, management of chronic diseases, hospital administration, and medical services such as payment applications to a geographically larger and even remote demographics but also at much reduced costs [11]. More groundbreaking IoT healthcare innovations are looming over the horizon and the integration of communication and network technologies could prove to be a game changer in the healthcare domain as they harness the myriad of possibilities in pervasive and cutting-edge technologies in which complex, intelligent medical devices, sensors, implants or wearables [12] could be developed with the capabilities to store health records and which could be used to save a patient's life during emergency situations [13, 14]. Thus, by observing the huge potential and opportunities for the growth and expansion that could cause astounding paradigm shifts in the healthcare domain, the IoT can be further exploited in order to address the emerging needs of healthcare providers as well as elevating the standard and quality of patients receiving improved clinical care in the future.

However, the risks of information security incidents and vulnerabilities have also seen an alarmingly steady rise [15] whereby healthcare information in particular, is being increasingly targeted by criminals [15]. There have been many published studies on IoT security and privacy issues and challenges [15, 16] and these problems remain at large especially for IoT-based medical devices [16–18] following the endless string of disclosures on major information breaches [19, 20] that have occurred in many healthcare organisations globally. A significant number of researches have shown [17, 18, 20] that these vulnerabilities have opened avenues to criminals who devise new methods to attack, steal, destroy or manipulate the medical devices and its configurations including the network structure misconfigurations, software design flaws, third-party vulnerabilities, absence of tamper proofing, coding defects, authentication, access control, secure middleware, policy enforcement and etc. [17, 18, 20]. Severe ramifications could occur for the patients if such malicious attacks exposes their health information, presenting a pronounced risk and harmful effects to the patients' privacy and safety [17]. Personal clinical information is critical in the healthcare sector and the confidentiality, integrity and availability of healthcare information continues to be a grave concern to all stakeholders within the ecosystem. Therefore, it is imperative to ensure that healthcare information is always safeguarded against both malicious and non-malicious attacks and its security and privacy must be given utmost priority at all times.

4 Research Methods

A preliminary investigation study was carried out for the purpose of information gathering and to gauge the feedback and opinions from selected participants regarding the IoT information security non-compliance issues in healthcare organisations.

4.1 Field Settings

The preliminary investigation involved interviewing respondents who are experts and are currently or previously based in healthcare organisations or facilities and have exposure in healthcare information security issues, healthcare systems and operations, and healthcare information security management. The selection criteria for selecting the participants was each of them must have related working experience in their respective field of expertise for a minimum number of two years.

4.2 Qualitative Research: Semi-structured Interviews

The qualitative research design was considered a suitable approach for the preliminary investigation study 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 [21] The rationale behind the selection of the semi-structured interview method was twofold: Firstly, to gauge the feedback and opinion of the respondents regarding the non-compliance issues that were faced by the healthcare organisations and secondly, to investigate on the potential mitigation measures and how to deliver them. The semi-structured interview method was applied as it provided flexibility with the interview questions, thus allowing an unhindered, detailed line of questioning based on the interviewees' responses. 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 [21]. Before the interviews were conducted, an interview guide was provided to all the respondents to give them an overall idea about the preliminary investigation study as well as the interview procedure.

4.3 Participants' Background

In total, sixteen individuals who are experts in healthcare information security from a spectrum of organisations were selected for the preliminary investigation study. Two participants were from well-established medical IT solutions companies, and fourteen were from various prominent private hospitals in Malaysia. The participants' job designations among others, were several clinical academicians, healthcare information systems managers, medical doctors, health inspectors, nursing staff, hospital IT administrators and etc. while their work experiences ranged from two to forty years. 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.

4.4 Data Collection

Three research questions were formulated as follows

i. What are the issues faced by your healthcare organisation pertaining to IoT information security compliance?
ii. What are the possible reasons behind the occurrence of these issues?
iii. Which potential measures can be enforced in order to cultivate and increase the compliance levels?

The first question is oriented to identify which issues could lead to IoT information security compliance being compromised in private healthcare organisations. Realizing that these issues could possibly be stemmed from multiple causes, a second question was formulated as we were also interested to find the reasons behind information security non-compliance. Finally, a third question was framed as we also wanted to identify potential measures that can be enforced to raise the levels of compliance in healthcare organisations from independent points of view.

5 Initial Findings

The preliminary study sought to ascertain if the healthcare organisations in Malaysia faced challenges and issues in achieving information security compliance in managing IoT-based medical devices and networks. Based on the findings, the study also suggests several potential means of increasing the compliance levels among the employees of healthcare organisations within the Malaysian private healthcare sector.

5.1 Derivation of Information Security Compliance Issues

According to the findings shown in Table 1, most of the issues and challenges that were identified and revealed as the main causes of non-compliance which have contributed to the lack of proper enforcement of the information security policies, standards and governance in the healthcare organisations are inexorably linked to the Human or People dimension i.e. the healthcare employees rather than technology, as supported by findings from earlier researches [22, 23]. Secondly, through the responses, it has been generally discovered that many of the healthcare employees based in different healthcare organisations with varying job categories and positions tend to share similar workplace attitude and behavioural characteristics or problems as displayed in Table 1, which leads to non-compliance of information security policies.

Table 1. Identification of information security non-compliance issues in Malaysian private healthcare organisations

Poor work attitude	Lack of management commitment	Malicious intentions
Irresponsible behaviour	Overloaded with job tasks	Habits
Lack of IS awareness	Lack of education and training	Unintentional errors or threats
Information security fatigue	Absence of organisational measures	Compromise
Negligence	Unclear policy guidelines	Non-stringent IS policies
Ignorance	Outdated enforcement of policies	Emotions
Ego/ Superiority/ Pride/ Annoyance	Non-malicious causes	Absence of IS work culture
Lack of motivation	Social Norms	Lack of ethical conduct
Lack of disciplinary actions	Lack of employee monitoring	Lack of safeguards and defences
Lack of involvement	Fear towards technology (phobia)	Carelessness
Poor integrity	Resistance towards change	Complexity of policies

6 Discussion

Information security compliance is not a new phenomenon nor is it an emerging trend but it has only been in the last several years that it has started to gain significant acknowledgement across the major industry players globally. The healthcare domain especially would be exposed to a plethora of vulnerabilities and breaches if compliance of information security is overlooked, increasing the security and privacy risks and threats to healthcare organisations. Therefore, it is imperative that information security compliance must be well-managed through implementing a practical, precautionary approach to privacy and security, which should include technological and more importantly, organisational controls in order to create a valuable strategy that healthcare organisations can apply to manage the threats and breaches.

6.1 Organisational Measures

Among the many administrative measures that were proposed in order to motivate and engage behaviour for achieving compliance, every single respondent collectively agreed that the most crucial one would be a comprehensive and continuous Security Education and Training (SETA) which requires that all healthcare employees be given sufficient education and training [7, 22] especially on IoT information security which ought to continue periodically [6, 22] throughout the employment tenure at their respective organisation. In corresponding to their answers, we would like to further suggest that the organisation should identify the different category of users and learners so that the SETA package could be customized accordingly to better suit the needs and requirements of each group.

Besides providing SETA, we would like to suggest that the employees who suffer from information security fatigue and phobia to undergo motivational talks and counselling sessions with the aim of overcoming their resistance towards compliance of information security. Issues dealing with human attitude and behaviour are never easy to handle and these motivational talks and counselling sessions ought to be conducted discreetly and appropriately as not to offend them further as it could cause unnecessary embarrassment or more consternation among themselves due to the sensitivity of the issue. The counsellors must be very wise, cautious and patient in dealing with this category of end-users so that they would be able to overcome their intense dislike, exasperation or fear with computer systems and devices.

Additionally, having a responsible management which is committed to the information security compliance cause is also another crucial factor in motivating and persuading the healthcare employees [24]. 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. 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 [6]. The rewards-based measures would increase the motivation and compliance levels [6, 25] while the sanctions-based measures would instill a sense of caution and could determine the success rate of compliance [6, 25].

Other measures that were proposed and discussed during the interview sessions were providing effective technology support from the IT team, efficient communication channels and allowing more room for employee empowerment.

6.2 Technological Measures

The findings from the preliminary investigation also revealed that the healthcare infrastructure requirements for IoT needs to be strengthened or re-evaluated to ascertain its capability in mitigating the latest malware and other types of cyber-attacks that could exploit or cause damage to the IoT-based medical information.

Therefore, many of the respondents proposed that an advanced malware protection software be installed to ensure the organisation is able to fend itself from internal or external malicious attacks on the IoT medical devices [26]. Another safeguard mentioned by the respondents would be the embedding of a hospital Virtual Private Networks (VPNs) within a private Access Point Network (APN) to add another layer of security for the IoT medical devices [5]. The majority of the respondents also mentioned that healthcare organisations should consider implementing a cutting-edge IoT device encryption technology as an option to safeguard sensitive information such as Personally Identifiable Information (PII) [5, 27] which is often used by healthcare organisations and their working associates such as insurance companies, legal firms and etc. Despite being a relatively simple measure, having robust encryption standards would still create difficulties in decrypting the stored information should the device gets hacked [27]. The micro-segmentation of information through sandboxing is also another measure that was stated by the interview respondents. Sandboxing is considered as the most secured state for a networked IoT medical device because it is completely isolated in a “sandbox” which means the location where it is locked down and secured by the network it’s attached to [26].

Furthermore, the respondents also suggested that a two-factor authentication controls on IoT medical devices and security servers such as locking the device with biometrics as well as using a passcode should be enforced to mitigate inadequate security controls. Additionally, the healthcare organisations could also apply remote/automatic lock and wipe capabilities after an excessive number of incorrect login attempts on a particular IoT medical device has been made [27]. A baselining strategy could also be implemented to capture the analytics of access control mechanisms information flow in order to detect unauthorized intrusions [28]. According to the respondents, this measure can help eliminate the Denial of Service (DoS) attacks on the information servers of the IoT platform.

Other potential technological measures that were identified and mentioned by the respondents also included keeping security patches up to date, replace aging legacy networks as they can create significant security vulnerabilities, have appropriate logging and monitoring controls, conduct more frequent vulnerability assessments and penetration testing, perform frequent security risk analysis, testing product data security features, enlisting third-party audits of security procedures [5, 26–28] and etc. Having many layers of technical security measures or safeguards can create enough barriers to help reduce information security threats and vulnerabilities and makes hacking into the system complicated and time-consuming. IoT provides the medical industry with immense benefits in many ways, especially in delivering more efficient healthcare service to the patients as well as reducing expenses. Thus, the healthcare providers and their affiliates should ensure that information security policies and procedures must be enforced strictly in order to protect the healthcare information as well as to achieve compliance.

7 Conclusion

Based on the preliminary investigation that was conducted, this paper presents the initial findings on the causes of information security non-compliance among the employees of the private healthcare organisations in Malaysia. Potential organisational and technological measures as safeguards were further identified by the respondents and proposed to be enforced in order to help raise compliance levels and reduce information security threats and vulnerabilities. Further research could include an empirical study with bigger demographics, as well as, to study the best organisational measures that can effectively lead to better awareness and commitment among the healthcare employees.

References

1. Roman, D.H., Conlee, K.D., Sachs, G.: The Digital Revolution Comes to US Healthcare: Technology, Incentives Align to Shake Up the Status Quo, Internet of Things, vol. 5 (2015)
2. Mora, H., Gil, D., Munoz Terol, R., Azorin, J., Szymanski, J.: An IoT-based computational framework for healthcare monitoring in mobile environments. Sensors (Basel, Switzerland) **17**(10), 2302 (2017). https://doi.org/10.3390/s17102302
3. Dimitrov, D.V.: Medical Internet of Things and Big Data in Healthcare. Healthc. Inform. Res. **22**(3), 156–163 (2016). https://doi.org/10.4258/hir.2016.22.3.156
4. Garg, A.: The Internet of Things: impacts on healthcare security and privacy, Litmos Healthcare Division, Berkeley Research Group (2016). http://www.litmos.com/wp-content/uploads/2016/06/webinar-IoT.pdf
5. Al-Siddiq, W.: IoT innovator, Internet of Things news, medical technology and IoT: mitigating security risks (2018). http://iotinnovator.com/medical-technology-and-the-internet-of-things-addressing-and-mitigating-security-risks/
6. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS Q. (2010). https://doi.org/10.2307/25750704
7. Pham, H.C., Pham, D.D., Brennan, L., Richardson, J.: Information security and people: a conundrum for compliance. Aust. J. Inf. Syst. **21** (2017)
8. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**, 2787–2805 (2010). https://doi.org/10.1016/j.comnet.2010.05.010
9. Gil, D., Ferrandez, A., Mora-Mora, H., Peral, J.: Internet of Things: a review of surveys based on context aware intelligent services. Sensors (Basel, Switzerland) **16**(7), 1069 (2016). http://doi.org/10.3390/s16071069
10. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., Aharon, D.: The Internet of Things: mapping the value beyond the hype. McKinsey Global Institute, June 2015
11. Wortmann, F., Fluchter, K.: Internet of Things—technology and value added. Bus. Inf. Syst. Syst. Eng. **57**(3), 221–224 (2015)
12. Kulkarni, A., Sathe, S.: Healthcare applications of the Internet of Things: a review. Int. J. Comput. Sci. Inf. Technol. **5**(5), 6229–6232 (2014)
13. Aliverti, A.: Wearable technology: role in respiratory health and disease. Breathe **13**(2), e27–e36 (2017). https://doi.org/10.1183/20734735.008417
14. Jeong, J.-S., Han, O., You, Y.-Y.: A design characteristics of smart healthcare system as the IoT application. Indian J. Sci. Technol. **9**(37) (2016). https://doi.org/10.17485/ijst/2016/v9i37/102547
15. Mamlin, B.W., Tierney, W.M.: The promise of information and communication technology in healthcare: extracting value from the chaos. Am. J. Med. Sci. **351**(1) (2016)
16. Qi, J., Yang, P., Xu, L., Min, G.: Advanced Internet of Things for personalised healthcare system: a survey. Pervasive Mob. Comput. **41** (2017). https://doi.org/10.1016/j.pmcj.2017.06.018
17. Baker, S.B., Xiang, W., Atkinson, I.: Internet of Things for smart healthcare: technologies, challenges, and opportunities. IEEE Access **5**, 26521–26544 (2017). https://doi.org/10.1109/ACCESS.2017.2775180
18. Harbers, M., van Berkel, J., Bargh, M.S., van den Braak, S., Pool, R., Choenni, S.: A conceptual framework for addressing IoT threats: challenges in meeting challenges. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)

19. Talkin Cloud: IoT past and present: the history of IoT, and where it's headed today (2016). http://talkincloud.com/cloud-computing/iot-past-andpresent-history-iot-and-where-its-headed-today?page=2
20. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in IoT: the road ahead. Comput. Netw. 146–164 (2015)
21. Creswell, J.W.: Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th edn. SAGE Publications, Inc., Thousand Oaks (2013)
22. Safa, N.S., Von Solms, R., Furnell, S.: Information security policy compliance model in organisations. J. Comput. Secur. **56**(C), 70–82. Elsevier Advanced Technology Publications Oxford, UK
23. Fernandez-Aleman, J.L., Sanchez-Henarejos, A., Toval, A., Sanchez-Garcia, A.B., Hernandez-Hernandez, I., Fernandez-Luquec, L.: Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int. J. Med. Inform. **84**, 454–467 (2015)
24. Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: a literature review. Int. J. Inf. Manag. **36**, 215–225 (2016)
25. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34** (3), 523–548 (2010)
26. CISCO Whitepaper. Cybersecurity in the age of medical devices, connected & protected: an industry point of view (2017). https://www.cisco.com/c/dam/m/digital/healthcare/cybersecurity-in-the-age-of-medical-devices.pdf
27. Wright, KOnramp: Control the risks of IoT and BYOD in healthcare—part II (2017). https://www.onr.com/blog/control-the-risks-of-iot-and-byod-in-healthcare-part-ii/
28. Blowers, M., Iribarne, J., Colbert, E., Kott, A.: The future Internet of Things and security of its control systems (2016). https://arxiv.org/ftp/arxiv/papers/1610/1610.01953.pdf