Journal of Theoretical and Applied Information Technology
30th April 2023. Vol.101. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SOFTWARE SECURITY READINESS MODEL FOR REMOTE WORKING IN MALAYSIAN PUBLIC SECTORS: CONCEPTUAL FRAMEWORK

HALIMATON HAKIMI[1], MASSILA KAMALRUDIN[2], RAIHANA SYAHIRAH ABDULLAH[3], MOHD FAIZAL ABDOLLAH[3], SAFIAH SIDEK[4] , NIK SUKI[5], DEWI OCTAVIANI[1], AERVINA MISRON[6]

[1]Lecturer, School of Computing, Asia Pacific University, Kuala Lumpur, Malaysia
[1]Researcher, Faculty of Information Technology and Communication (FTMK), University Teknikal Malaysia Melaka, Malaysia
[2]Professor, Innovative Software System and Service Group (IS3), Universiti Teknikal Malaysia Melaka,Malaysia
[3]Doctor, Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka, Malaysia
[4]Associate Professor, Innovative Software System and Service Group (IS3), Universiti Teknikal Malaysia Melaka, Malaysia
[5]Lecturer, School of Technology, Asia Pacific University, Kuala Lumpur, Malaysia
[6]Lecturer, Faculty of Business and Technology, UNITAR International University, Selangor Malaysia

Corresponding E-mail: [2]massila@utem.edu.my,

ABSTRACT

Resulting from the COVID-19 pandemic, which requires mankind to practice social distancing, companies and government agencies do not have any options but to send their workers home and practice remote working. With very limited guidance, workers are required to work remotely by utilizing various software facilitated by Internet. The increased dependence on the cyberspace opens up the organization to become highly vulnerable to cyber threats/crimes, which may affect their performance. Hence, organizations need to manage their cyber risk by ensuring that they are capable to manage software security. Therefore, this study aims to propose a new software security readiness model that is able to measure the level of organizational readiness for workers working remotely. The readiness model enables the organizations to take proactive actions for continuously improving their weaknesses related to cyber threats. Furthermore, the model can be used as guidance to develop policy for the organization specifically and for the country (Cybersecurity Malaysia) for ethical use of digital technologies especially for remote working.

Keywords: *Software Security, Readiness Model, Remote Working, Public Sector*

1. INTRODUCTION

Malaysia government need to provide effective software security infrastructure and environment for better public sector especially during COVID-19 pandemic. Impact from the COVID-19 pandemic, which required mankind to practice social distancing, companies and government agencies do not have options but to send their workers home and practice remote working. The pandemic has particularly lit a fire and created an air of urgency in this “remote migration”. Along with this active ambition there must also be an urgency to support and assist common local communities with software security needs. The change to more prevalence and acceptance for work from home positions is necessary and beneficial but it must not leave business processes, personal data or critical infrastructure at risk. This is usually due to underfunding or ignoring software security all together. Working from home can end up just as bad or worse with employees using their own unsecure network to conduct critical work processes and handle sensitive data. The increased dependence on the cyberspace opens up the organization to become highly vulnerable to cyber threats/crimes, which may affect organization performance. In this case, one of the ways for

organizations to manage their cyber risk is by ensuring that they are ready and aware of software security. Despite having information security policy in place, the readiness of organizations in ensuring the awareness among the workers and their compliance with software security while working remotely is still questionable, thus exposing them to several security threats. Further, this policy is too restrictive, lacking the aspect of software security. Hence, it is necessary to consider readiness perspective to model software security public sector in order to meet requirements in the better manage cyber threats from occurring. The identification of the readiness model enables the organizations to identify the weakness that needs improvements; hence they can proactively manage any possible cyber threats from occurring. In fact, the security readiness model generalized to the public sectors can help to create a more strategic cyber risk management in future. Whereas many studies of network and technology readiness focused solely on technology aspect, there has been a lack of model that include management and human components to build the complete picture of an organization's software security readiness. Further, although there are several studies and works on software security, these studies tend to focus on addressing the security issues during the development of software and studies that managing software securities from the end-users are still scarce. It needs to be properly managed to public organization when they experience the security measures.

Therefore, there is a needed to develop a software security model that is able to measure the level of readiness among workers working remotely. The readiness model enables the organizations to take proactive actions for continuously improving their weaknesses related to cyber threats.

The purpose of this study to identify the factors of software security in public organization which leads to be design of a new proposed software security readiness model for remote working in public organization. Hence, the coverage of this study is within the context of software security and readiness model in public organization .

The rest of this paper is organized as follows: Section II presents the background and motivation. Section III presents the conceptual framework of software security readiness model in this paper. Section IV concludes the paper with some discussions about software security readiness model and future works.

2. BACKGROUND AND MOTIVATION

2.1 Software Security, Cyber Risk Management and Remote Working

Software security refers to the protection of the programs that are either bought from an outsider vendor or created in-house by users. It concerns with the methods used for controlling software used to run the operating system or utility software [4]. The focus of software security is to proactively protect assets from attacks that will result in losses. Organizations that lack awareness of software security may suffer from cyberthreats which may affect the performance of the organizations and lead to losses. Hence, operating in the vulnerable cyber environment, it is crucial for organizations to be equipped with software security. Unlike most of the studies on software security that focus on addressing security at the beginning of the software process, built into the design, implementing it in the coding and verifying it during testing [8] this research aims to develop the capability of software security among end-users.

The increasingly development of IoT devices and the existence of sophisticated attackers have resulted in the emergence of cyber risks. Cyber risks refer to the operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems, and it can be classified according to the activity (e.g., criminal and non-criminal), the type of attack (e.g., malware, insider attack, spam, distributed denial of service), and the source (e.g., terrors, criminals, government) [7]. Therefore, workers working from home should have some knowledge about cyber privacy and cybersecurity, in which failing to do so may damage the reputation of the organization.

When working remotely, employees are no longer working directly under the security of the organization. Communication is mainly conducted via mobile applications or other channels, which increases the possible sources of security threats [11]. Possible issues related to the heavily dependent on the technology are the cyber threats that may happen when working remotely are phishing scams that result in numerous data breaches, virtual private network that could not handle everyone working from home, issues of security and data privacy and many others [1][11] claim that enhancing security depends on changing

the beliefs, attitudes, and behaviours of individuals and groups. According to [5], a breach in security does not generally result from a flaw in the technical system but it can be a result of noncompliant employee behaviour. Based on their study of the non-compliant behaviour, they identified two main factors of non- compliance which are individual perception climate and self-efficacy. Therefore, a study of software security readiness among workers working from home is necessary to address the threats of cyber risks faced by organizations.

An analysis of selected studies from 2015 indicate that there are four main security aspects related to organizational securities which are i) information security [4][15][22], ii) security policy [3][4][15][[22] , iii) security training [3][4][15][[22]and iv) security awareness [3][4][15][[22]. For the purpose of this study, these factors will be considered as the antecedents for software security readiness.

2.2 Readiness Model/Index

Readiness referred to the state of being fully ready to engage in a specific activity. It highlights the importance of timing, state and specificity of an activity, in relation to psychological, behavioral and structural preparedness of the organization [16]. In this study, readiness is considered as the state of capabilities for continuous improvement. According to [24], the measurement of readiness is crucial as it: i) provides pre-assessment of the organization's tangible and intangible capabilities, ii) indicates where the capability building is required and iii) reduces the risk of failure.

To date, readiness model or indexes related to digital technology that have been developed are such as, the the Global Digital Index [6]. The purpose of these readiness indexes is to measure the state of capabilities of certain effort across the globe and they can be used as benchmark for future improvement in future. Specifically, the Global Digital Index was developed to help nations understand their position in the uptake of digitalization, to measure the progress the nation has made towards digital maturity and demonstrate areas of strengths and provide guidance as to how they can invest to improve their overall readiness. Another example is the Government AI readiness index, which was developed to provide an overview of the government's readiness to use AI. This index facilitates global comparisons as well as the ability to track government progress in this area overtime. Focusing on examining how ready the government to implement AI based on four generic clusters, which are governance, infrastructure and data, skills and education and innovative practices of the government and public services.

Studies on readiness tend to relate to the use of ICT at the organizational level. There are works to related to readiness model encompassing cloud security risk and readiness [40], cybersecurity readiness index [14] and e-readiness assessment model [25]. [40] developed a readiness model that enables cloud services customer to tackle the needs across several different security area, such as compliance, governance or data protection as well as allow the identification of potential risk factors related with the use of cloud computing. However, the focus on this study is on cloud services rather than on information security. [4] proposed a web-based model that compute cyber security readiness index [CRI] for hospital based on the four pillars of cybersecurity: people, process, policy and technology. Due to the vulnerability to attacks, there is a need to develop a model that will help hospital perform self-assessment in determining its readiness to fight the cyber-attack menace. Although this study has relevance to information security and cybersecurity, it is contextualized within healthcare industry. [25] proposed e-readiness assessment model, by defining e-readiness as the availability of the necessary physical infrastructure, bandwidth, reliability and affordable prices, access to information [software and information system], availability of devices required to access information [hardware and network availability and survivability]; degree to which the ICT master plans and policies cope with the vision of an organization, the security level adopted by the organization and the human resource to use and manage these resources for the implementation of e-governance . This work tends to focus on the organizational level towards the implementation of e-governance, deemphasize on readiness or awareness of software security among workers. Drawn from the selected studies above, studies related to software security readiness model are still lacking, and this is the gap this research aims to address.

2.3 The Factors to Determine Readiness of Software Security in Public Organization.

There are many works done to enhance the security in public organization. For example, [26]

have developed a new approach for ICT security readiness checklist for developing countries. They are conducted quantitative approach to measure the effectiveness of security for developing countries. The measurement item focus in information security which is confidentiality, integrity and availability. However this research more focusing on developing countries rather than focus on organization.

Next, Upadhyaya [27] developed E-government security readiness assessment for developing countries. In this studies, they are use mixed research method in which both qualitative and quantitative methods and techniques are used in the overall study. They are use two sets of questions were prepared. The first set was targeted for IT department heads, and security experts or system administrators because they manage all the information systems functionalities including its security while the security experts or system administrators make sure that the systems are functioning as per the required policy, procedures, organization's requirement, etc. The second set was a general security related questions targeted for any employee of that organization to understand whether information systems users in the organizations to know the awareness of IS security, policies and procedures, training they received, etc. Questionnaires that were targeted to the IT department heads were designed based on the ISO audit checklist customized and ICT security readiness checklist addressing the main components to assess the IS security readiness and audit of a given organization. Even though, this study focusses on the security readiness in organization. But they are doing not focus on public organization.

Mijnhardt [18] developed Information Security Focus Area Maturity for Small Medium Enterprise SME information security as cornerstone in the development of an assessment too for tailor-made, fast, and easy-to-use information security advice for SMEs. They evaluate the model with the expert it ICT. They evaluate based on these two important factors in the security which are information security and security policy. This another seven previous studies also mentioned that information security and security policy are important in the security of organization [13][14][22][15]. This work describes exploratory research into the field of adaptive IS assessments targeted at SMEs. They performed a systematic literature review and assembled a total of 75 organizational factors. By grouping factors and removing factors not adhering to set criteria, we identified a long list of 26 OCs for IS in SMEs. For each of these OCs, the levels of measurement were defined and a number of iterative interviews were held. Even though this study focus on the security maturity but they more focusing on the measurement security in SME rather than public organization.

Furthermore, [2] was conducted survey to assess the information security posture within Omani public sector organization, as well as the Omani manager's attitude towards Security. In the survey, they targeted four dimensions of security in public organization which are 1. Organization's Information Security Policy 2. Organization's compliance with IS best practices 3. Information Security Training and Awareness 4. Managerial attitude towards Information Security. These four dimensions were specified as aspects of Information Security. The survey was conducted anonymously and was disseminated electronically via the Internet to all participants. Questions were written in Arabic and English to accommodate the native language and working language of participants. However, this study those do not cater on the security readiness in the public organization.

[13] was discussed on the security issues in Saudi Arabia Small Organization. The studies more emphasize that the precise awareness of information security policy, its aspects and practices is a significant point that organizations must pay attention to prevent potential security threats. However, some Saudi organizations lack the security awareness. They represents some previous studies that were conducted to evaluate the state of policy, information security awareness and security training [28] and application in a Saudi organization. They consider a small Saudi organization to perform a case study, to audit its state and describe the possible risk scenarios that may take place. Most information about the company was gathered by interviewing its CEO. The audit found five possible risk scenarios, named lack of security policy, personal information leakage from the website, the risk of damage of the CEO's device and two scenarios related to outsourcing companies.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Therefore, they provided some recommendations to the audited organization which may serve other organizations that have the same characteristics, which are adopting and documenting a comprehensive security policy and procedures from beginning stages of a company, ensure that the employees are aware of these documents and the required practices to secure sensitive information. In addition, introduce a mechanism to ensure that security controls are met and to secure personal information transmitted over their website and recommending to regularly checks that the website is bugs free. Additionally, recommends considering more security details on the outsourcing contracts and involve a specialized attorney on it. Also, prefer short-term out- sourcing contracts and take possible alternatives third-party companies into consideration as a precaution.

In the nutshell, the comparison of all above-mentioned related works and the summarization of factor to determine readiness of security in public organization in Table 1.

Based on Table 1, we found 21 paper published between 2014-2020 that discussed on the topic of security readiness model in public organization. For each of the papers, we identified the factor of software security. In the nutshell, the comparison of all above-mentioned related works and the

Table 1: Factors Of Software Security In Public Organization

Author	Factor									Domain
	Information Security			Security Policy	Infrastructure	Security Processed	Security Training	Culture	IT Knowledge	
	Availability	Integrity	Confidentiality							
[26]	x	x	x							IT
[27]				x	x	X				E-Government
[18]	x	x	x	x						SME
[5]	x	x	x	x						Cloud System
[29]	x	x	x	x	x					IT
[2]				x			x		x	Public organization
[4]	x	x	x	x	x					Public Organization
[3]				x	x	X	x			Organization
[30]				x			x			Organization
[3]				x			x		x	Organization
[28]				x			x		x	Education
[31]				x						Organization
[32]				x			x	x	x	Organization
[33]								x		Organization
[34]									x	SME
[35]	x	x	x	x						Organization
[36]	x	x	x	x			x		x	
[37]	x	x	x	x			x		x	Services organization
[15]	x	x	x	x			x		x	Learning Organization
[38]							x		x	Organization
Total	**9**			**16**	**4**	**2**	**10**		**9**	

summarization of factor to determine readiness of software security in public organization in Table 1.

Altogether, five important factors were identified from a total of 21 studies to the factors involved in software security in public organization. Based on the Table 1 above, we found that Security Policy and Security Training is most important factor which account 16 studies and 10 studies. This is followed by IT knowledge and information security nine studies. The rest of this studies brief of description of these findings.

As a conclusion, although Security policy, Security Training and Information Security is the most concerned factor identified in this review, the weightage of applying the factor influence is different. It shows that, only six factors of software security which are IT knowledge, Security Training, Security Policy, Information Security, Technology Infrastructure are gained more crucial and attention in security of public organization. Therefore, in Table 2, we explain in general and operational definition of six factors of security in public organization.

Table 2: Operational Definition Of Software Security Factor

Factor	Operational Definition	Sources	Underlying Theory
Security Policy	System security policies and procedures that specify or control how often a system or organization offers security services in order to secure vulnerable and vital system resources are known as security policies and procedures.	[18]	Theory of planned behaviour
Information Security	Confidentiality, integrity, and availability of information are mostly protected from unauthorized access, use, disclosure, alert, inspection and recording or damage through the practice of information security.	[4]	CIA theory
Security Awareness Training	Formal process for educating employees about computer security	[2]	ISA Theory SETA
IT knowledge	Employees of an organization's workforce have knowledge and attitudes regarding defending the organization's physical assets, as well as its information assets, in addition to their own personal assets. Formal security awareness training is required by many firms with all employees when they first begin working for the company and on a regular basis afterward, generally once a year.	[3]	Knowledge theory
IT Infrastructure	Infrastructure software is a type of enterprise software or program specifically designed to help business organizations perform basic tasks such as workforce support, business transactions and internal services and processes. The most common examples of infrastructure software are database programs, email and other communication software and security applications.	[19]	Institutional theory
Trust	Trust is a willingness to be vulnerable to the actions of another person or people.	[17]	Technology Acceptance Model (TAM)
Reliability	Reliability is defined as the probability that a given system operates properly for a specified period of time. As a companion definition to reliability, availability of a system for its users is defined as the relative frequency that the system works.	[39]	Technology Acceptance Model (TAM)
Software Security readiness	The level of an organization’s awareness, preparedness and commitment to prevent and combat security attack	[10]	TOE Theory

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.0 CONCEPTUAL FRAMEWORK

Figure 1 shows the conceptual framework of software security readiness model for remote working in public sector. The model is developed based on the literature review. This conceptual framework is extended from TOE framework and readiness framework. The developments of the model start with determination of factors of security readiness of smart governments. The purpose of developing a new software security readiness model for remote workers as reference for organization to measure the software security readiness of organization for level security among remote working employee in organization. Based on the literature review conducted, we found that there are seven factors of software security for remote workers which are: 1) IT knowledge, 2) trust, 3) security training, 4) security policy, 5) information security, 6) IT infrastructure and 7) reliability. In the study we are proposed two new factor which are 1) Trust and 2) . The first seven (7) factors are derived from the literature review, while the later two factors are based on the perception of the researchers which is reliability and usability.

The model consists antecedents of the software security readiness comprise three main aspects which are i) individual, ii) organizational and iii) technology. The three aspects are considered as the active agents to build the capacity for software security readiness and they are interrelated to each other. For the individual aspect has three constructs which are IT knowledge and Trust. Th organization aspect there are three constructs which are security policy, security training, and information security. The technology aspect has two constructs which are infrastructure, and reliability.

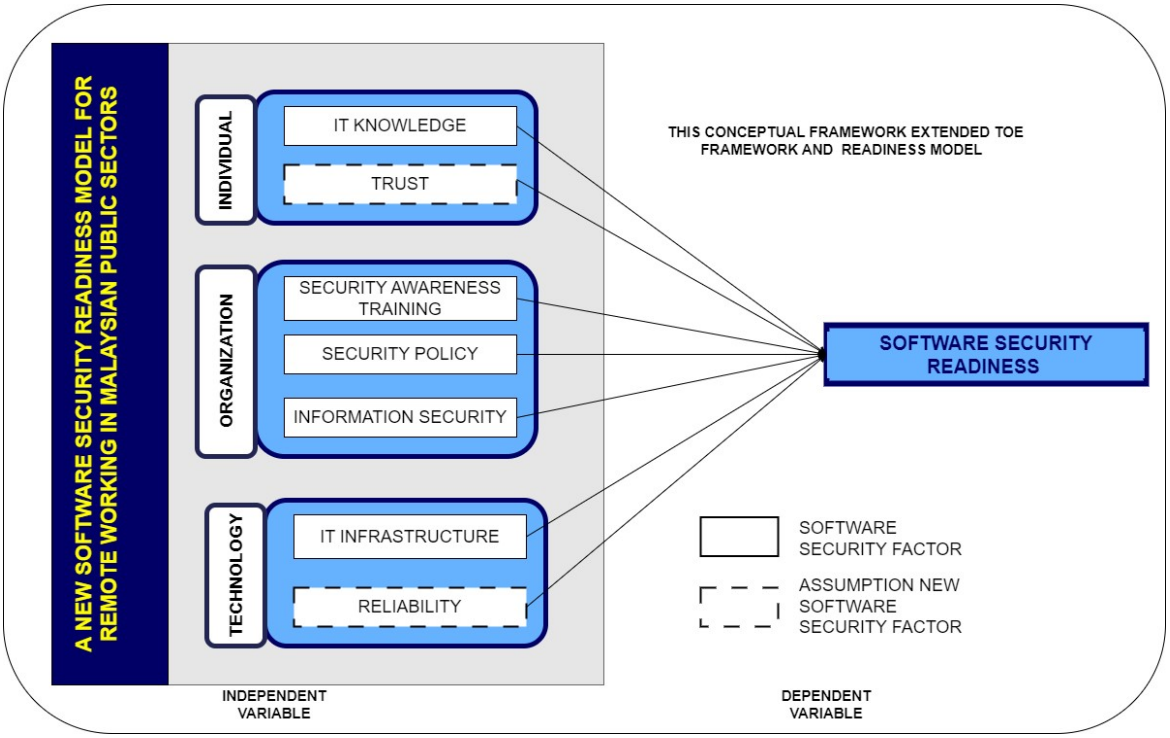

Figure 1: The Proposed Conceptual Framework Software Security Readiness Model (Soserm)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Formulation Research Hypothesis

Factor	Hypothesis		Description
IT Knowledge	H1	H_1	The self-attitude factor has significant relationship to software security readiness
		H_0	The self-attitude factor has no significant relationship to software security readiness
Trust	H2	H_1	The IT knowledge factor has significant relationship to software security readiness
		H_0	The IT knowledge factor has no significant relationship to software security readiness
Security Training	H3	H_1	The trust factor has significant relationship to software security readiness
		H_0	The trust factor has no significant relationship to software security readiness
Security Policy	H4	H_1	The security training factor has significant relationship to software security readiness
		H_0	The security training factor has no significant relationship to software security readiness
Information security	H5	H_1	The security policy factor has significant relationship to software security readiness
		H_0	The security policy factor has no significant relationship to software security readiness
Infrastructure	H6	H_1	The information security factor has significant relationship to software security readiness
		H_0	The information security factor has no significant relationship to software security readiness
Reliability	H7	H_1	The infrastructure factor has significant relationship to software security readiness
		H_0	The infrastructure factor has no significant relationship to software security readiness

Motivated from the gaps described by the literature and determine factor of software security readiness in section 2, we propose to overcome the gaps through proposing a software security readiness model for remote working in public sector. This software security readiness model will employ the concept of readiness model design as per described in Section 2. This is because it found that readiness model able to incorporate human perspective and technology for better change in remote working in public organization. Figure 1 shows the conceptual framework proposed for this study. As shown in Figure 1, the software security readiness model for remote working Based on the conceptual framework presented in Figure 1, the hypotheses to be tested in this study presented in Table 3 below.

4.0 CONCLUSION AND FUTURE RESEARCH DIRECTION

This study contributes on new factor of security readiness for public organization in Malaysia, organization can use this model for reference in developing the successful public organization.

The intention was to develop security readiness model to help guide the top management in the public organization to measure readiness of security according employee expectation. For future work, we will evaluate and validate the security readiness model with our potential respondent that working in public organization at Malaysia.

Several limitations of this study should be considered in interpreting the findings. The empirical study context is limited to organization in Malaysia. The factors investigated in this study could have different levels of importance in different contextual settings, and future studies

investigating the same factors could consider organizations from other developing countries.

REFERENCE

[1] Ahmad, Tabrez, Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity (April 5, 2020).
[2] Al-Izki, Fathiya, and George RS Weir. "Management attitudes toward information security in Omani public sector organisations." In 2016 Cybersecurity and Cyberforensics Conference (CCC), pp. 107-112. IEEE, 2016.
[3] Almubayedh, Hanine, and Rizwan Ahmad. "Ethnopharmacological uses, phytochemistry, biological activities of Debregeasia salicifolia: a review." Journal of ethnopharmacology 231 (2019): 179-186.
[4] Antoniou, G.S., 2018, April. A Framework for the Governance of Information Security: Can it be Used in an Organization. In SoutheastCon 2018 (pp. 1-30). IEEE.
[5] Chan, M., I. Woon, and A. Kankanhalli. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior." Journal of Information Privacy and Security 1 (3): 18–41.
[6] Cisco. (2020). Cisco Global Digital Readiness Index 2019, White paper, available at https://www.cisco.com/c/en/us/about/csr/research-resources/digital-readiness.html Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474–491.
[7] Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, *17*(5), 474-491.
[8] Firesmith, D.G. (2012) Engineering Safety- and Security-Related Requirements for Software-Intensive Systems. The 11th IASTED International Conference on Software Engineering (SE 2012) in Crete, Greece on 18 June 2012.
[9] Fong, S., Dey, N., & Joshi, A. (Eds.). (2020). ICT Analysis and Applications. Lecture Notes in Networks and Systems. doi:10.1007/978-981-15-0630-7
[10] Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, p.102726.
[11] Hazari, S., Hargrave, W., & Clenney, B. (2008). An Empirical Investigation of Factors Influencing Information Security Behavior. Journal of Information Privacy and Security, 4(4), 3–20.
[12] Holt, D.T., Bartczak, S.E., Clark, S.W., and Trent, M.R. 2007. "The Development of an Instrument to Measure Readiness for Knowledge Management," Knowledge Management Research & Practice (5:2), pp 75-92.
[13] Kamalrudin, M., Hakimi, H., Abdollah, M.F. and Hardi, R., 2022, November. SSRINDEX tool: An automated tool to measure level of software security readiness index for remote working during Covid-19 pandemic. In AIP Conference Proceedings (Vol. 2658, No. 1, p. 020001). AIP Publishing LLC.
[14] Kiplimo, A.E. (2018). A web-based model to determine cybersecurity readiness index for hospitals towards adoption of e-health, unpublished dissertation
[15] Kirlappos, I., Parkin, S. & Sasse, M.A., 2015. " Shadow Security " as a tool for the learning organization. In SIGCAS Computer & Society, pp. 29–37.
[16] Lokuge, S., Sedera, D., Grover, V., & Dongming, X. (2018). Organizational readiness for digital innovation: Development and empirical calibration of a construct. Information & Management. doi:10.1016/j.im.2018.09.001.
[17] Mayer, R.C., Davis, J.H. and Schoorman, F.D., 1995. An integrative model of organizational trust. Academy of management review, 20(3), pp.709-734.
[18] Mijnhardt, F., Baars, T. and Spruit, M., 2016. Organizational characteristics influencing SME information security maturity. Journal of Computer Information Systems, 56(2), pp.106-115.
[19] Roldán Salgueiro, J.L., Real, J.C. and Sánchez Ceballos, S., 2018. Antecedents and consequences of knowledge management perfomance. the role of IT infrastructure.
[20] Usman, M., Liu, Y., Zhang, J., Ghani, U. and Gul, H., 2022. Why do employees struggle to thrive in the workplaces? A look

at the impact of abusive supervision. Personnel Review, 51(1), pp.77-97.
[21] Oxford Insight (2019), Government Artificial Intelligence Readiness Index 2019, available at https://ai4d.ai/index2019/
[22] Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. Industrial Management & Data Systems, 111(4), 570–588
[23] Hakimi, H., Kamalrudin, M., Akmal, S., Yusop, N. and Sidek, S., 2018. Determination of trust requirements attributes for developing acceptable autonomous car. The Turkish Online Journal of Design, Art and Communication, Special Edition, pp.2571-2579.
[24] Yen, H.R., Wang, W., Wei, C.-P., Hsu, S.H.-Y., and Chiu, H.-C. 2012. "Service Innovation Readiness: Dimensions and Performance Outcome," Decision Support Systems (53:4), pp 813- 824.
[25] Gupta, A., Shakya, S., & Marasini, S. (2015). E-Readiness Assessment for Ministries of Nepal for Implementation of e-government. In 2015 International Conference on Data Mining, Electronics and Information Technology (DMEIT'15) (pp. 10-11).
[26] Tarimo, C. N. (2006). ICT security readiness checklist for developing countries: A social-technical approach (Doctoral dissertation, Institutionen för data-och systemvetenskap (tills m KTH)).
[27] Upadhyaya, P., Shakya, S., & Pokharel, M. (2012, November). E-government security readiness assessment for developing countries: Case study: Nepal Govt. organizations. In 2012 Third Asian Himalayas International Conference on Internet (pp. 1-5). IEEE.
[28] Sari, P. K., & Nurshabrina, N. (2016, April). Factor analysis on information security management in higher education institutions. In 2016 4th International Conference on Cyber and IT Service Management (pp. 1-5). IEEE.
[29] Kautsarina, K., Rafizan, O., Setiawan, A. B., & Sastrosubroto, A. S. (2017). Information and communication technology service industry development in Indonesia. Journal of Telecommunications and the Digital Economy, 5(3), 50-82.
[30] Felipe, F. D., Acevedo, E. M., & Sanchez, M. M. (2017, August). Evaluating informatics security in an organization: The minimal distance method. In *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)* (pp. 1-3). IEEE.
[31] De Lange, J., Von Solms, R., & Gerber, M. (2016, May). Information security management in local government. In *2016 IST-Africa Week Conference* (pp. 1-11). IEEE.
[32] Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". Journal of Enterprise Information Management, 27(5), 644-667.
[33] Singh, J. (2014, March). Real time BIG data analytic: Security concern and challenges with Machine Learning algorithm. In 2014 Conference on IT in Business, Industry and Government (CSIBIG) (pp. 1-4). IEEE.
[34] Savolainen, R. (2017). Information sharing and knowledge sharing as communicative activities. *Information Research: an international electronic journal*, *22*(3), n3.
[35] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, 70-82.
[36] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225.
[37] Joshi, C., & Singh, U. K. (2017). Information security risks management framework–A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128-137.
[38] Weixun Li, W., Chung Man Leung, A., & Yue, W. T. (2023). WHERE IS IT IN INFORMATION SECURITY? THE INTERRELATIONSHIP AMONG IT INVESTMENT, SECURITY AWARENESS, AND DATA BREACHES. *MIS Quarterly*, *47*(1).
[39] Jung, I., Quan, W., Yu, J., & Han, H. (2023). Are you ready for robot services? Exploring robot-service adoption behaviors of hotel-goers. International Journal of Hospitality Management, 109, 103404.
[40] Ferreira, L. P. T. (2017). Cloud security risk and readiness (Doctoral dissertation)