An Awareness Model for Software Security in Smart Government: Conceptual Framework

Salem Alfalasi, Institute Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

*Suriati Akmal, Doctor, Institute Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Massila Kamalrudin, Professor, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Halimaton Hakimi, PhD, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Corresponding:

suriati@utem.edu.my

Article Info
Page Number: 1350-1365
Publication Issue:
Vol. 71 No. 3s2 (2022)

Abstract: The need for this study is grounded on attempting to fill knowledge and empirical gaps surrounding the effectiveness of the software security awareness model in addressing security challenges among smart government stakeholders. By attempting to evaluate the effectiveness of the application of the software security awareness model in smart cities, added knowledge can be contributed towards recommendations of smart solutions to security concerns. It is a fact that the rise of globalization and digitization has propelled the development of smart cities worldwide but there are still a few software security challenges that needs to be considered especially in security awareness. On top of that, this study aims to provide the awareness model for software security in smart government. The proposed conceptual model for evaluating stakeholder's awareness to use software security system in smart cities of UAE. The proposed model will improve the security of software that implemented in smart cities of UAE.

.**Keywords:** Awareness Model, Software Security, Smart Government, Conceptual framework

Article History
Article Received: 28 April 2022
Revised: 15 May 2022
Accepted: 20 June 2022
Publication: 21 July 2022

I. Introduction

Modernization and urbanization are the most common dimensions of the concept of smart city. In the last decade, there has been an increased growth of technological advancements such as in the aspect of information and communication technologies (ICTs) and digital technologies. As such, these advancements in information and communication technologies, the rise of the internet and the growth of digital technologies led to the development of smart cities particularly in developing economies (Mohanty, Choppali and Kougianos, 2016).

Over the last decades, city governments have increasingly experienced complex problems as influenced by certain. The UAE is currently moving towards the promotion of smart governance. In line with this, software security is one of the important elements of ensuring effective implementation of smart governance. Smart government stakeholders including the citizens (users), politicians, industries, startup businesses, entrepreneurs and private and public organizations among others can have significant influence in the effectiveness of smart government adoption in the country. According to Almuraqab, et al (2017), there are certain factors that can pose as barriers to the effectiveness of UAE smart governance. For one, quality awareness of software security in smart governance is considered as an issue in the adoption of smart governance in UAE (Almuraqab, et al, 2017). In particular, the same authors noted that lack of awareness concerning privacy and security of the information of users is a current issue in the adoption of smart government services in UAE. Users are among the stockholders impacted directly by smart governance and therefore it is important to address awareness on software security among smart government stakeholders. As such, the conceptual model proposed in this study can be used to evaluate and improve the awareness of stakeholders with regard to the quality of software security being adopted in smart government projects in the UAE.

The rest of this paper is organized as follows: Section II presents the background and motivation. Section III presents the awareness model for software security proposed in this paper. Section IV concludes the paper with some discussions related on awareness model for software security and future works.

II. Background and motivation

A. Awareness Model for Software Security

A security awareness program provides financial benefits to many organizations. Major benefits include organizations information security performance, values, beliefs, attitude and action of the organization members. All the users are responsible for the protection of information; it is not only the responsibility of information security people of the company. Information security means protecting information and information systems from unauthorized access, unauthorized use and disclosure. Many of the organization and Universities are still vulnerable from human attitude threats.

Apart from the said components, frameworks can be developed or consulted in organizing a security awareness program. Among these frameworks is the Information Security Awareness Program (ISAPM) of Maqousi, Balikhina and Mackay (2013). The said model is established in seven core blocks and has been adopted based on the concepts of increasing users' security awareness level. These concepts were also proven to educate users, which served as one best practice to increase their awareness levels. The ISAPM model is shown in the figure below.

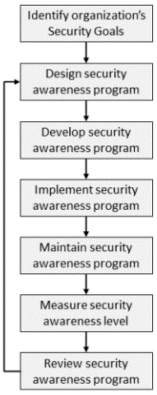
Identify organization's Security Goals
Design security awareness program
Develop security awareness program
Implement security awareness program
Maintain security awareness program
Measure security awareness level
Review security awareness program

Figure 1: Information Security Awareness Program (ISAPM) of Maqousi, Balikhina and Mackay (2013)

As explained by Maqousi, Balikhina and Mackay (2013), the framework begins with identifying the security goals of the organization, which covers interviewing computer staff and the staff responsible for managing and running computer and Internet services. The main goal or aim of the said interviews is to identify and understand the security goals, while considering the nature of the organization, the users and the customers of the services, the employees' expertise and qualifications, and the methods of IT security employed and existing policies and processes. The second stage is the design process, which is primarily concerned on identifying the needed program elements that must be included in the security awareness program. Certain guidelines are included in this element, such as awareness training workshops, booklets, posters, and online forums that allow users to interact, alert and news sections, online surveys and statistics. The said system should easily be accessed and must have clear content, apart from being interactive through diverse multimedia. The third tier in the framework is highlights the development of a security awareness program, which can be performed through range of web-based development tools, such as ASP.NET or PHP. Deciding on the tool to be used must be based on the concept of a Content Management System (CMS), in order to provide online platform that enable users' contributions. In this sense, the content of the system would be enriched and more so emphasized the user's responsibilities in raising security awareness to all.

The fourth tier pertains to the implementation process that covers choosing one of three ways in running and distributing the program. This could be a part of the organization's website, administrative tools or as separate website. Maqousi, Balikhina and Mackay (2013) proposed to integrate the program in the organizational website as his will increase the program's visibility and make it more accessible to all users of the organization.

The fifth tier in Maqousi, Balikhina and Mackay's (2013) framework referred to the maintenance process, which intends to define a process of consistently maintaining a program by providing updated and suitable content. Ensuring proper maintenance requires organizations to employ skilled staff that is qualified to run and maintain the program.

The sixth step is the measuring process that is concerned on assessing and measuring current users' security awareness levels. Such process should be made on a regular basis, either online or offline. A number of periodical reports and statistical data are to be generated and published so it could be made available to any authorized users, via the main security awareness website. (Maqousi, Balikhina & Mackay, 2013; Davoudizadeh, 2020)

The last tier is reviewing the security awareness program, which is performed by the administrative and technical staff or the reviewing team. This is conducted online. The team will review all the reports and statistics collected from the measuring process. They will also approve or define a new set of requirements to be included in the program. The recommendations of the reviewing team will eventually be forwarded to the development process for further actions. This would form the closed system. (Maqousi, Balikhina & Mackay, 2013; Farah Kordmahaleh, 2021)

An organization can also consider looking at the toolkit approach as part of organizing the security awareness program. As what Korovessis et al. (2017) underscored, the toolkit approach can help in raising awareness levels of the people or the stakeholders about information security. The toolkit as well serves as the basis for general technology users to comprehend the challenges associated with secure utilization of information technology. The toolkit format can also aid in evaluating the current knowledge and identify the weaknesses and insufficiencies in acquiring the needed knowledge to become competent and confident users. It is essential to note that the toolkit is composed of pre-assessment, main e-learning unit and post-assessment. The goal of the pre-assessment unit is to identify the knowledge of participants on certain information security topics and identify if additional training is needed. Pre-assessment comes in the form of multiple choice questions to be answered by the user. Meanwhile, the primary goal of the main e-learning unit is introduce participants with important daily information security skills and help in protecting their computers, mobile devices and data from attacks. It is also designed to provide interactive learning experience. The post-assessment quiz would determine if a passing or failing score is attained. (Korovessis et al., 2017).

The authors [7] examine the level of ethical and security awareness among IT students. Satisfactory level of awareness among IT students was found out in this survey. Through the questionnaire survey they found that the female students are more conscious about security and ethics awareness when compared to male students.

III.Development of conceptual framework

To construct a software security awareness model, an understanding of existing awareness models and frameworks are essential. A review of the existing frameworks and security awareness measures are essential to develop a new conceptual model. The comprehensive review of software security awareness and framework was conducted and based on the identification and the findings of the review; proposed an software security awareness model. The objective and constructs of each study in the information security area leads to develop a conceptual model. This review has also included a questionnaire assessment of information security to assist in the development of information security awareness model.

Table 1: Summary of proposed constructs in software security awareness research

Authors	**Factor influencing awareness of software security**																					
	Training	**Policy**	**Trust**	**Communication**	**Employee**	**Firm Structure &**	**Virtual interactivity**	**System quality**	**Information content**	**Rewarding activities**	**Campaigns**	**Perceived Risk**	**Appointment of**	**Information Sharing**	**Security Website**	**Management and**	**Security**	**Building**	**Security knowledge**	**Security Attitude**	**Security**	**Product quality**
Mahesh, Prabhuswamy, & Mamatha (2010)	1				**1**																	
(Al-Shami et al., 2021)									1													
Kahsay, Osanna & Durakbasa (2007)		1																				1
Hussain,			1	1	**1**	1															**1**	

Authors	**Factor influencing awareness of software security**																					
	Training	**Policy**	**Trust**	**Communication**	**Employee**	**Firm Structure &**	**Virtual interactivity**	**System quality**	**Information content**	**Rewarding activities**	**Campaigns**	**Perceived Risk**	**Appointment of**	**Information Sharing**	**Security Website**	**Management and**	**Security**	**Building**	**Security knowledge**	**Security Attitude**	**Security**	**Product quality**
Abba & Leleu-Merviel (2006)																						
Sadikoglu & Olcay (2014)					**1**	1															**1**	
Barreda, et al (2015)							1	1	1	1												
(Al-shami et al., 2022)									1													
Shabbir, et al											1											

Authors	**Factor influencing awareness of software security**																					
	Training	**Policy**	**Trust**	**Communication**	**Employee**	**Firm Structure &**	**Virtual interactivity**	**System quality**	**Information content**	**Rewarding activities**	**Campaigns**	**Perceived Risk**	**Appointment of**	**Information Sharing**	**Security Website**	**Management and**	**Security**	**Building**	**Security knowledge**	**Security Attitude**	**Security**	**Product quality**
(2010)																						
(Doheir, Basari, Elzamly, Yaacob, & Al-shami, 2019)																			**1**			
Hashemi and Hajiheydari (2012)												1										
Sulaiman et al., (2012)											1		1	1	1				**1**			

Authors	**Factor influencing awareness of software security**																					
	Training	**Policy**	**Trust**	**Communication**	**Employee**	**Firm Structure &**	**Virtual interactivity**	**System quality**	**Information content**	**Rewarding activities**	**Campaigns**	**Perceived Risk**	**Appointment of**	**Information Sharing**	**Security Website**	**Management and**	**Security**	**Building**	**Security knowledge**	**Security Attitude**	**Security**	**Product quality**
Ebenehi, et al, (2018)						1										1	1	1	**1**	**1**		
Agyekum et al., (2016)	1															1	1		**1**	**1**		
Ibrahim et al., (2011)																		1				
Yunus and Yahya (2011)																						
Kazaras et al. (2012)					**1**				1											**1**	**1**	

Authors	**Factor influencing awareness of software security**																					
	Training	**Policy**	**Trust**	**Communication**	**Employee**	**Firm Structure &**	**Virtual interactivity**	**System quality**	**Information content**	**Rewarding activities**	**Campaigns**	**Perceived Risk**	**Appointment of**	**Information Sharing**	**Security Website**	**Management and**	**Security**	**Building**	**Security knowledge**	**Security Attitude**	**Security**	**Product quality**
Altabbakh et al., (2015)	1																		**1**	**1**	**1**	
Total	3	1	1	1	**4**	3	1	1	2	1	2	1	1	1	1	2	2	2	**4**	**4**	**4**	1

The main purpose of this review in to construct a conceptual model for software security awareness through the finding of the review in Table 1. Table1 shows related works about the factors influencing software security awareness. Based on the review conducted, this study identifies the most common factors found in literature as shown in Table 3. The effectiveness of the application of the software security awareness model in developing smart city in smart government of UAE that will be measured using the variables **knowledge, attitude, and consciousness**. These variables can be used as grounding framework for determining the effectiveness of the application of software security awareness model towards achieving knowledge sharing and continuous improvement thereby improving Smart government in UAE.

The model for awareness of software security awareness model is shown in Figure 2. From the Figure 2 security awareness is part of any organization security. Every organization software security depends on the external and internal factors. Through the proper awareness solution organization’ information and software security system are preserved from inside and outside threats.

Information security policy mainly focuses on information management and training on general staff. Software security policies should be promoted in a top-down manner to meet the requirements and it should be reviewed at planned intervals. Because of the lack of awareness about the importance of information security among students and staff in the organization the policies are often reviewed to protect the information.

Knowledge management helps individual people to do their job in an efficient way through better decision making and problem solving. This will be helpful to keep people up to date and minimize the opportunities for computer fraud. In an organization level, users become upgraded when their experience and knowledge were shared. Knowledge management will encourage people to give new ideas and innovations and rewarding them accordingly.

Development of software security model needs to be educating people. The software security training and awareness program covers recent issues in security and needs motivations to improve and enhance the awareness about software security. Organizations need to work consciously towards creating a brand image. Positive brand image leads to organizations gain and negative brand image leads to bad impression in user's mind. Software security methods are used to protect the software from unauthorized access. Methods are derived to understand the principles and rules of different situations. The responsibility covers how an individual handle software carefully and must be trained to become aware of the loopholes. The development of software security awareness needs the combination of training and campaigning to increase the understanding of software security.

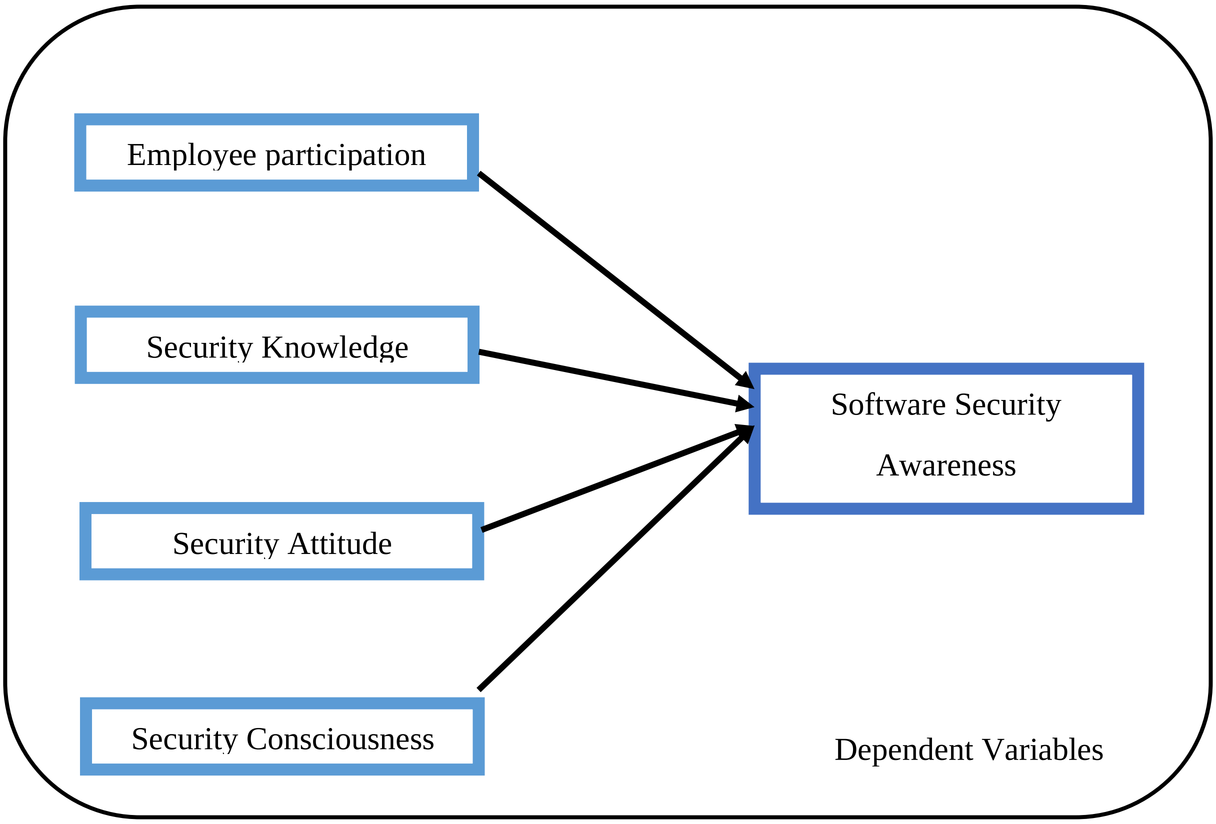

Figure 2: The proposed conceptual framework for software security awareness model

IV.Conclusion

Lack of awareness and less priorities about software security leads to this software security awareness model. This model identifies the further actionable step for the improvement of the society. Software security awareness should be the first priority in the development of Internet service providers. The existing literature review provides suggestions and guidelines on how to prevent our Information's from the external and internal factors. These literature analyses have not provided a clear idea or understanding to develop a conceptual model. This is an initiative to identify what factors constitute a conceptual awareness model. The proposed model influences the order of security awareness. In order to achieve this goal, questionnaire survey will be conducted to develop the software security awareness model in organizations. Additionally, qualitative interviews will also be included to identify the awareness. These will assist to minimize the external factors which will affect the security awareness. This is not implemented in any organization or university. The implementation of this model would be the future work of this paper. During the implementation the rankings and the constructs place might be changed depending on the organization.

V.Acknowledgement

The authors would like to thank the Universiti Teknikal Malaysia Melaka.

VI.References

1. Aliyu, A. A., Singhry, I. M., Adamu, H. and Abubakar, M. M. (2015). Ontology, Epistemology and Axiology in Quantitative and Qualitative Research: Elucidation of the Research Philosophical Misconception. Proceedings of The Academic Conference: Mediterranean Publications & Research International on New Direction and Uncommon Vol. 2 No. 1. 22nd December, 2015- University of Agric, Abekuta, Abekuta, Ogun State, Nigeria
2. Allin, B. (2018). How to Implement a Security Awareness Program at Your Organization. Retrieved from < https://www.threatstack.com/blog/how-to-implement-a-security-awareness-program-at-your-organization>
3. Al-shami, S. A., Aldahmani, S., Kamalrudin, M., Al-kumaim, N. H., Mamun, A. Al, Al-shami, M., & Jaber, M. M. (2022). A Model of Motivational and Technological Factors Influencing Massive Open Online Courses ’ Continuous Intention to Use. Sustainability (Switzerland), 14(15), 9279.
4. Al-Shami, S., Al-Hammadi, A. H., Hammadi, A. Al, Rashid, N., Al-Lamy, H., & Eissa, D. (2021). Online social networking websites in innovation capability and hotels’ performance in Malaysia. Journal of Hospitality and Tourism Technology, 12(1), 72–84.
5. Ashworth, R. E., McDermott, A. M. and Currie, G. (2019). Theorizing from Qualitative Research in Public Administration: Plurality through a Combination of Rigor and Richness. Journal of Public Administration Research and Theory, 29(2), 318-333
6. Association for Computing Machinery (ACM) et al. (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Retrieved from <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>
7. Axelsson, K. and Granath, M. (2018). Stakeholders' stake and relation to smartness in smart city development: Insights from a Swedish city planning project. Government Information Quarterly, 35, 693-702
8. Axelsson, K. and Granath,M. (2018). Stakeholders' stake and relation to smartness in smart city development: Insights from a Swedish city planning project. Government Information Quarterly, 35(4), 693-702

9. Banerjee, C. and Pandey, S. K. (2010). Research on software security awareness: problems and prospects. ACM SIGSOFT Software Engineering Notes, 35(5), 1-5
10. Banerjee, D., Muraka, P. D. and Banerjee, A. (2013). An Improvised Software Security Awareness Model. International Journal of Information, Communication and Computing Technology, 11(2), 43-48
11. Bernardo, M. R. M. (2017). Smart City Governance: From E-Government to Smart Governance. In: Entrepreneurial Development and Innovation Within Smart Cities. IGI Global
12. Beyer, A. & Westendofr, C. (2010). "How to Establish Security Awareness in Schools, ISSE 2009 Securing Electronic Business Processes." Information Security Solutions Europe Conference (2009), pp.177-186.
13. Bharathi, S. and Suguna, J. (2014). A Conceptual Model To Understand Information Security Awareness. International Journal of Engineering Research & Technology (IJERT), 3(8), 402-405.
14. Bogolea, B. & Wijekumar, K. (2017). Information Security Curriculum Creation: A Case Study, pp.55-65.
15. Caird, S. P. and Hallett, S. H. (2019). Towards evaluation design for smart city development. Journal of Urban Design, 24(2), 188-209
16. Cappelli, D.M., Trzeciak, R.F. & Moore, A.P. (2006). "Insider Threats in the SDLC, A study conducted by CERT, U.S. Secret Service, CSO Magazine, Program, Software Engineering Institute, Carnegie Mellon University." Retrieved on from www.cert.org/archive/pdf/sepg500.pdf
17. Castelnovo, W., Misuraca, G. and Savodelli, A. (2015). Smart Cities Governance: The Need for a Holistic Approach to Assessing Urban Participatory Policy Making. Social Science Computer Review, 34(6), 1-16
18. Chua, W. F. (1986). Radical Developments in Accounting Thought. The Accounting Review, 66(4), 601-632
19. Clark, M. I., Berry, T. R., Spence, J. C., Nykiforuk, C., Carlson, M. and Blanchard, C. (2016). Key stakeholder perspectives on the development of walkable neighbourhoods. Health Place, 16(1), 43-50.
20. Vanitha, D. D. . (2022). Comparative Analysis of Power switches MOFET and IGBT Used in Power Applications. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 01–09. https://doi.org/10.17762/ijrmee.v9i5.368
21. Cohen, L., Manion, L. and Morrison, K. (2000). Research Methods in Education. London: Routledge
22. Comte, A. (2009). The Positive Philosophy of Auguste Comte, Vol. 1. New York: Cosimo
23. CSO Magazine (2010). 2010 Cyber Security Watch Survey: Cybercrime increasing faster than some company defenses. Retrieved from <https://resources.sei.cmu.edu/asset_files/News/2010_100_001_53454.pdf>
24. Cui, L., Xie, G., Qu, Y., Gao, L. and Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. IEEE, 6, 46134-46145

25. Davoudizadeh R, Hosseini Seno S A. Analyzing Advantages and Benefits of Information Technologies in Organizations. sjis. 2020; 2 (1) :7-19, URL: http://sjis.srpub.org/article-5-56-en.html
26. Doheir, M., Basari, A. H., Elzamly, A., Yaacob, N., & Al-shami, S. S. A. (2019). The New Conceptual Cloud Computing Modelling for Improving Healthcare Management in Health Organizations. International Journal of Advanced Science and Technology, 28(1), 351–362.
27. Farah Kordmahaleh A, Farah Kordmahaleh H. The Impact of Supply-Chain and Quality Management Procedures on the Innovation Performance of Small and Medium Enterprises. sjamao. 2021; 3 (1) :9-16, URL: http://sjamao.srpub.org/article-7-90-en.html
28. Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2008). Management Research, Third Edition. London: SAGE Publications
29. Eremia, M., Toma, L. and Sanduleac, M. (2017). The Smart City Concept in the 21st Century. Proceedia Engineering, 181, 12-19
30. Flynn, M., Rao, A. K. and Gashi, D. S. (2018). Smart Cities Funding and Financing in Developing Economies. Deloitte
31. Ghosh, P. and Mahesh, T. R. (2015). Smart City: Concept and Challenges. International Journal on Advances in Engineering, Technology and Science, 1(1), 25-27
32. Gray, D. E. (2004). Doing Research in the Real World. London: SAGE Publications.
33. Guenduez, A. A., Singler, S., Tomczak, T., Schedler, K. and Oberli, M. (2018). Smart Government Success Factors. Swiss Yearbook of Administrative Sciences, 9(1), 96–110
34. Hancock, B. (1998). An Introduction to Qualitative Research. Nottingham. UK: Trent Focus Group, Division of General Practice, University of Nottingham.
35. Hancock, B., Ockleford, E. and Windridge, K. (2009). An Introduction to Qualitative Research. The NIHR RDS for the East Midlands / Yorkshire & the Humber (Leicester)
36. Harvey-Jordan, S., & Long, S. (2001). The process and the pitfalls of semi-structured interviews. Community Practitioner, 74(6), 219-221.
37. Howard, M. & Lipner, S. (2006). The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software. Redmond, WA: Microsoft Press.
38. Ijaz, S., Shah, M. A., Khan, A. and Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. International Journal of Advanced Computer Science and Applications, 7(2), 612-625
39. Jayasena, N., Mallawaarachchi, H. and Waidyasekara, A. (2012). Stakeholder Analysis For Smart City Development Project: An Extensive Literature Review. MATEC Web of Conferences, 266(2), 1-6
40. Deepak Mathur, N. K. V. . (2022). Analysis &amp; Prediction of Road Accident Data for NH-19/44. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 13–33. https://doi.org/10.17762/ijrmee.v9i2.366
41. Keegan, S. (2009). Qualitative Research: Good decision Making Through Understanding People, Culture and Markets. London: Kogan Page Ltd.
42. Ken van Wyk, C. (2012). Training and Awareness. Retrieved from < https://www.us-cert.gov/bsi/articles/best-practices/training-and-awareness/training-and-awareness>

43. Korovessis, P., Furnell, S., Papadaki, M. & Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. Journal of Cybersecurity Education, Research and Practice, 2(5), 1-34. Retrieved from https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/5
44. Kruger, H., Drevin, L. & Steyn, T. (2007). "Email Security Awareness — a Practical Assessment of Employee Behaviour." In IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, Futcher, L., Dodge, R., (Eds.). Boston: Springer, pp. 33–40.
45. Kwon, M., Jacobs, M.J., Cullinane, D., Ipsen, C.G. & Foley, J. (2012). Educating cyber professionals: A view from academia, the private sector, and government. IEEE Security and Privacy 10(2), 50-53.
46. Lopez-Quiles, J. M. and Bolivar, P. R. (2018). Smart Technologies for SmartGovernments: A Review of TechnologicalTools in Smart Cities. In: M.P. Rodríguez Bolívar (ed.), Smart Technologies for Smart Governments. Springer International Publishing AG
47. Maqousi, A., Balikhina, T. & Mackay, M. (2013). An effective method for information security awareness raising initiatives. International Journal of Computer Science & Information Technology (IJCSIT), 5(2), 63-72.
48. Marquardt, K. (2017). Smart Services – Characteristics, Challenges, Opportunities and Business Models. 11th International Conference on Business Excellence 2017, At Bucharest
49. Matrooshi, S. R. O. K. (2016). The Challenges of Developing Smart Services Projects in the United Arab Emirates. Thesis. The British University in Dubai
50. Meijer, A., Pedro, M. and Bolivar, R. (2015). Governing the smart city: a review of the literature on smart urban governance. International Review of Administrative Sciences, 82(2), 392–408.
51. Agarwal, D. A. . (2022). Advancing Privacy and Security of Internet of Things to Find Integrated Solutions. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 05–08. https://doi.org/10.17762/ijfrcsce.v8i2.2067
52. Mohanty, S. P., Choppali, U. and Kougianos, E. (2016). Eveything You Wanted to Know About Smart Cities: The Internet of Things is the Backbone. IEEE Consumer Electronics Magazine, 5(3), 60-70
53. Monzon, A. (n.d.). Smart Cities Concept and Challenges: Bases for the Assessment of Smart City Projects. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7297938
54. Mutiara, D., Yuniarti, S. and Pratama, B. (2018). Smart Governance for Smart City. Earth and Environmental Science, 126, 1-11
55. Nam, T. and Pardo, T. A. (2011). Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. The Proceedings of the 12th Annual International Conference on Digital Government Research. ACM.
56. New, J., Castro, D. and Beckwith, M. (2017). How National Governments Can Help Smart Cities Succeed. Center for Data Innovation

57. Olzak, T. (2006). Strengthen Security with an Effective Security Awareness Program. Retrieved from http://adventuresinsecurity.com/ Papers/Build_a_Security_Awareness_Program.pdf
58. Paul, M. (2010). Software Security: Being Secure in an Insecure World. The International Information Systems Security Certification Consortium. Retrieved on from www.softwaremag.com/trk.cfm?uid=65
59. Pereira, G. V., Parycek, P., Falco, E., & Kleinhans, R. (2018). Smart governance in the context of smart cities: A literature review. Information Polity, 23(2), 1-20
60. Pierce, P. and Andersson, B. (2017). Challenges with Smart Cities Initiatives - A Municipal Decision Makers' Perspective. Proceedings of the 50th Hawaii International Conference on System Sciences.
61. Plas, J. M., Kvale, S. and Kvale, S. A. (1996). InterViews: An Introduction to Qualitative Research Interviewing. Sage Publications
62. Poepjes, R. and Lane, M. (2012). An Information Security Awareness Capability Model (ISACM). Proceedings of the 10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012.
63. Sarma, A., van der Hoek, A. & Redmiles, D.F. (2007). A Comprehensive Evaluation of Workspace Awareness in Software Configuration Management Systems IEEE Symposium on Visual Languages and Human-Centric Computing. IEEE, 23-26.
64. Security Innovation Europe (2018). Effective security awareness curriculum. Retrieved from < https://www.securityinnovationeurope.com/blog/page/effective-security-Awareness-Curriculum>
65. Smith, A.M. & Toppel, N.Y. (2009). “Northrop Grumman Corporation (2009): Case Study: Using Security Awareness to Combat the Advanced Persistent Threat.” Proceedings of the 13th Colloquium for Information Systems Security Education University of Alaska, Fairbanks Seattle, WA June 1 - 3, 2009, pp. 64-70.
66. Staller, K. M. (2010). Qualitative Research. In: Encyclopedia of Research Design, Vol. 3, Neil J. Salkind (Ed). Thousand Oaks, CA: Sage
67. Sujata, J., Saksham, S., Tanvi, G. and Shreya. (2016). Developing Smart Cities: An Integrated Framework. Procedia Computer Science, 93, 902-909
68. Thakurta, R. & Ahlemann, F. (2010). “Understanding Requirements Volatility in Software Projects – An Empirical Investigation of Volatility Awareness, Management Approaches and their Applicability.” Proceedings of the 43rd Hawaii International Conference on System Sciences – 2010, pp. 1-10.
69. Gill, D. R. . (2022). A Study of Framework of Behavioural Driven Development: Methodologies, Advantages, and Challenges. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 09–12. https://doi.org/10.17762/ijfrcsce.v8i2.2068
70. Abdul Rahman Ahlan, Muharman Lubis, “Information Security Awareness in University: Maintaining Learnability, Performance and Adaptability through Roles of Responsibility”, in proceedings of 7 th International Conference on Information Assurance and Security, IAS 2011, Melacca Malaysia, December 5-8, 2011.

71. Banerjee C., Arpita Banerjee, Murarka P.D., “An Improvised Software Security Awareness Model”, International Journal of Information, Communication and Computing Technology, Jagan Institute of Management Studies, New Delhi, Vol I, Issue II(July-Dec2013):ISSN 2347-7202.
72. Fadi A.Aloul, “The Need for Effective Information security Awareness”, Journal of Advances in Information Technology, Vol. 3, No.3, August 2012.
73. Hallvard Kjorvik, “Implementing and Improving Awareness in Information Security”, Thesis, University of Agder.
74. P. Modiya and S. Vahora, “Brain Tumor Detection Using Transfer Learning with Dimensionality Reduction Method”, Int J Intell Syst Appl Eng, vol. 10, no. 2, pp. 201–206, May 2022.
75. Ioannis Koskosas, Nikolas Sariannidis, nikolaos Asimopoulos, “A Survey in Project Commitment in the Context of Information Security”, Journal of Emerging Trends in Computing and Information Sciences, Volume 2, No 2, ISSN 2079-8407.
76. Kiran Kumar Kommineni, Adimulam Yesu Babu, “An approach for the Assessment of the Information Security and Its Measures”, International Journal of Soft Computing and Engineering(IJSCE), Volume 3, Issue-1, March 2013, ISSN:2231-2307.
77. Mansur Aliyu, Nahel A.O.Abdallah, Norjeem A.Lasisi, Dahir Diyar, and Ahmed M.Zeki, “Computer Security and Ethics Awareness among IIUM Students: An Empirical Study.
78. Ragul Rastogi, Rossouw von Solms,”Information Security Service Branding-beyond information security awareness”, Systemics, Cybernetics and Informatics, Volume 10, No.6, 2012, ISSN:1690- 4524.
79. Satish Kumar Er.,Amit Puri, “A Framework for Evaluation and Validation of Information Security Policy”, International Journal of Computers and Distributed Systems, Vol.No.1, Issue 3, October 2012, ISSN: 2278-5183.
80. Siponen T. Mikko, “Five Dimensions of Information Security Awareness”, Computers and Society, June 2001.
81. Toshihiko Takemura, “A Quantitative Study on Japanese Worker’s Awareness to Information Security Using the Data Collected by WebBased Survey”, American Journal of Economics and Business Administration 2(1):20-26,2010, ISSN:1945-5488.
82. Yogesh Kumar Mttal, Dr.Santanu Roy and Dr.Manu Saxena, “Role of Knowledge Management in Enhancing Information security”, International Journal of Computer Science, Issues, Vol. 7, November 2010, ISSN: 1694-0814.