An Awareness Model for Software Security in Smart Government: A Systematic Review

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: 54 - 66
Publication Issue:
Vol 71 No. 3 (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, software security awareness has become the main concern as it involves in creating stakeholder awareness by in developing smart cities. This study aims to determine the factors influence software security awareness in smart goverment and the related work awareness model. To do this, we have conducted systematic literature review to identify the factors that influence awareness of software security and to compare the existing awareness models.

Article History
***Article Received**: 12 January 2022*
***Revised**: 25 February 2022*
***Accepted**: 20 April 2022*
***Publication**: 27 May 2022*

Keywords: Awareness Model, Software Security, Smart Government.

I. Introduction

Over the last decades, city governments have increasingly experienced complex problems as influenced by certain social and technological factors. In response, a number of governments, mostly in developing countries, started to develop strategies that rely on advanced information and communication technologies (Lopez-Quiles and Bolivar, 2018). As such, these governments have been utilizing ICTs in pursuit of enhancing public sector services and meeting the needs and demands of stakeholders. This suggests that moving towards smart governance in cities require the use of ICTs in order to create interactive, participatory and information-based urban environments (Lopez-Quiles and Bolivar, 2018).

As highlighted by Guenduez, et al (2018), the key smart government success factors include institutional (i.e. IT infrastructure, digital awareness, political commitment, etc.), organizational (i.e. human resources, structure and processes, etc.) and leadership. Due to the strong reliance of smart governments on the use of advanced technologies, software security concerns are always apparent. Ijaz, et al (2016, p. 612) claimed that "With increasing boost in

urbanization, the concerns about economic restructuring, environmental issues, governance issues and public sector problems need to be dealt in a smarter approach". This means that security and privacy concerns are evident in smart cities. As such, Ijaz and colleagues asserted that the identification and classification of stakeholders of smart cities can aid in addressing security problems. In addition, Poepjes and Lane (2012) asserted that lack of awareness among involved stakeholders can also translate into security problems that can impact effective smart governance.

Moreover, Bharathi and Suguna (2014) noted that there are several risks and threats to software security including human errors, communication problems and technical problems among others. In relation to this, Ijaz, et al (2016) noted that there are a number of governance factors that can lead to security issues such as infrastructure, transport and utility among others. Therefore, to identify the security concerns in smart governance, it is important to understand the relationship among the different factors that influence information security. 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.

Therefore seeks to contribute to knowledge by bridging gaps in literature by exploring the application of software security awareness model for smart government. To the best knowledge of the researcher, there have been very few to no previous study of software security awareness model for smart government especially among stakeholder in United Arab Emirates (UAE).

This paper is organized into four main sections. After the introduction, the second section presents the methodology of the review. The third section presents the findings and discussion section. Finally, conclusion presented in the fourth section

II. Research methodology

We constructed a review protocol to search for the relevant studies based on Kitchenham systematic review approach. Our research focuses on a wider knowledge in software security awareness model for smart government. The approach of is divided into three phases, which are planning, conducting, and reporting. In the planning phase, we designed research questions as shown in Table 1. These research questions were designed to address the organization issues as aforementioned.

Table 1: Research questions

RQ1	What are the influential factors in the awareness model?
RQ2	What are the existing works in awareness model?

The review protocol activities are as shown in Figure 1. The purpose of adopting the review protocol is to ensure that all the relevant studies are captured for the analysis. The empirical studies were conducted by using search engines, namely, IEEE Xplore, ScienceDirect, Springer, Scopus, Google Scholar, and ACM Digital Library. The search keywords were used for different relevant topics to ensure that all related papers are included. (Awareness OR Awareness Model AND (Dimension OR Factors OR Element) AND (Software security OR software) AND (Approach OR Method OR Framework OR Model) AND (Smart Government) to collect all the relevant papers.

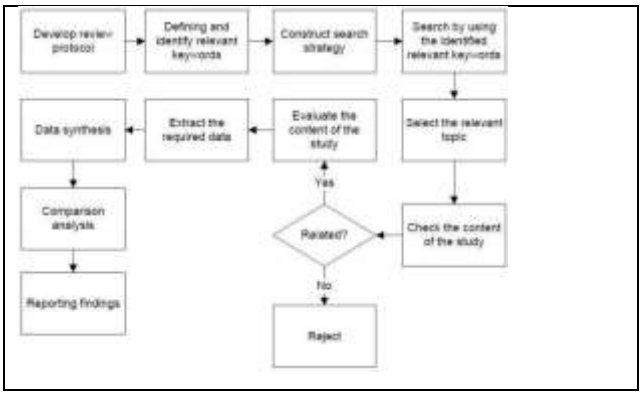

Figure 1: Review protocol process

We applied the inclusion and exclusion criteria as outlined in Table 2 to collect relevant studies. By analyzing the title, abstract, and conclusion of the primary identified studies, we eliminated any unrelated studies. After applying these steps, 30 studies were retained. Furthermore, we accessed and evaluated the articles by checking the content of the articles. Irrelevant studies were rejected at this stage and the relevant studies will be analysed. Out of 30 articles, only 15 articles were being considered for further review. The next phase was conducting the comparison analysis and reporting the analysis of the related works.

Table 2: Inclusion and Exclusion Criteria

Inclusion Criteria	**Exclusion Criteria**
Papers focusing on software security awareness model, security readiness model Papers focusing on frameworks, models, methods, and approach used in software security readiness model in smart government	Studies not related to the research questions Studies unclear

III. Findings and discussion

We found 19 papers published between 2014 and 2020 that discuss the topic of Awareness model of software security in smart government. For each of the paper, we identified the factors Influencing Awareness, type of contributions, and the domain of application of their approach. The results are presented in Table 3 and Table 4.

Table 3: Factor influencing awareness of software security

Authors	**Factor influencing awareness of software security**																			
	Training	**Policy**	**Trust**	**Communication**	**Employee participation**	**Firm Structure & Strategy**	**Virtual interactivity**	**System quality**	**Information content quality**	**Rewarding activities**	**Campaigns**	**Perceived Risk**	**Appointment of Spokesperson**	**Information Sharing with Public**	**Security Website**	**Management and maintenance**	**Security equipment/system**	**Building characteristic**	**Security knowledge**	**Security Attitude**	**Security Consciousness**	**Product quality**
Mahesh, Prabhuswamy, & Mamatha (2010)	1				**1**																	
Kahsay, Osanna & Durakbasa (2007)		1																				1
Hussain, Abba & Leleu-Merviel (2006)			1	1	**1**	1															**1**	
Sadikoglu & Olcay (2014)					**1**	1															**1**	
Barreda, et al (2015)							1	1	1	1												
Shabbir, et al (2010)											1											
Hashemi and												1										

Authors	Factor influencing awareness of software security																				
	Training	Policy	Trust	Communication	Employee participation	Firm Structure & Strategy	Virtual interactivity	System quality	Information content quality	Rewarding activities	Campaigns	Perceived Risk	Appointment of Spokesperson	Information Sharing with Public	Security Website	Management and maintenance	Security equipment/system	Building characteristic	Security knowledge	Security Attitude	Security Consciousness	Product quality
Hajiheydari (2012)																						
Sulaiman et al., (2012)											1		1	1	1				**1**			
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**	
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

Table 3 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.

Table 4: The summary of related works in awareness model

Authors	Domain	Method	Objective / Focus	Model Theory / Concept	Independent Variable	Dependent Variable	Mediating Variable	Moderating Variable	Tools & Technique	Region
Bogolea and Wijekumar (2017)	Government organization	Survey	Intent of acquiring information about their needs for employees with security training and areas of security considered of highest concern	Information security awareness	confidentiality, integrity, availability, authentication, auditing, threats and vulnerabilities , Legislation and industry standards	Information security awareness				

Authors	Domain	Method	Objective / Focus	Model Theory / Concept	Independent Variable	Dependent Variable	Mediating Variable	Moderating Variable	Tools & Technique	Region
Kahsay, Osanna & Durakbasa (2007)	Manufacturing	Survey	To examine quality awareness and developments and identify factors affecting product quality	Quality Management Model	Quality policy	Quality awareness		Product quality	Pareto Analysis, Ishikawa diagram	Ethiopia
Hussain, Abba & Leleu-Merviel (2006)	Automotive	Case study	To describe the components of quality awareness to implement quality practices in the organization	Quality Awareness Approach; Quality Awareness Triangle	Quality practice (Trust, communication, contribution)	Quality awareness		Company's strategies	Statistical Process Control (SPC) charts	France
Sadikoglu & Olcay (2014)	Not specified	Survey	To investigate impacts of TQM practices on different performance measures and the barriers and reasons of TQM practices	Total Quality Management Model	Performance outcome	Employee involvement / awareness / commitment		Firm structure and resources	Exploratory factor analysis and multiple regression analysis	Turkey
Barreda, et al (2015)	Online Social Networks (OSNs)	Survey	To propose and empirically test a theory-driven model of brand awareness in OSNs.	Theory-driven model of brand awareness in OSNs	Virtual interactivity, system quality, information content quality, and rewarding activities	Word of Mouth (WOM)	Brand Awareness		Brand awareness strategies	United States
Banerjee and Pandey (2010)	Not specified	Review	To propose of software security awareness	Software security awareness	• Training & Education • Awareness Campaign • Interview • Survey • Test & experiments • Games & stimulation • Awareness tool • Online community • Media & advertisement	Technique software security awareness	Software security		Review paper	Not specified
Hashemi and Hajiheydari (2012)	E-Commerce	Survey Questionnaires	Explore the most common online CKM tools and their effects on perceived risk in online purchase process and the influence of brand awareness as an important mediating factor.	Research Conceptual Model	Perceived Risk from CKM Tools	Knowledge about Internet, Risk Preference, Online Purchase Intention, Internet Preference	Brand Awareness		Likert Spectrum and Path Analysis	Tehran City
Azim Sulaiman, Mohd Najib Abd Rashid and Naim Mahyuddin, 2012 International Conference on Innovation and Technology for Sustainable Built Environment (ICITSBE 2012) *16 – 17 April 2012, Perak, MALAYSIA*	Public	Survey	To identify the level of fire safety awareness among the Malaysian public		Comprehensive Campaigns, Appointment of Spokesperson, Media Advertisement, Information Sharing with Public, Fire Safety Website, Education,	Governing Authorities				Malaysia

Authors	Domain	Method	Objective / Focus	Model Theory / Concept	Independent Variable	Dependent Variable	Mediating Variable	Moderating Variable	Tools & Technique	Region
Ebenehi, et al, 2018	Education building	survey	to develop an effective fire safety management framework for building fa-cilities in Malaysian	Fire Safety Management Audit Model	Management and maintenance, fire safety equipment/system, fire safety in building characteristic, user awareness & knowledge of fire safety, user's attitude to fire safety	Effective Fire Safety Management performance			Descriptive statistics	Malaysia
Computing Machinery (ACM) et al. (2017)	Cyber security	Propose a framework	Security Education, Training, and Awareness (SETA) programs	Cyber security	human security, alongside identity management, social engineering, social behavioral privacy and security, and personal data privacy and security	Cybersecurity infrastructure awareness			review	No specific

Authors	Domain	Method	Objective / Focus	Model Theory / Concept	Independent Variable	Dependent Variable	Mediating Variable	Moderating Variable	Tools & Technique	Region
V. Raja Sreedharan, R. Raju, R. Rajkanth & M. Nagaraj, (2016): An empirical assessment of Lean Six Sigma Awareness in manufacturing industries: construct development and validation, Total Quality Management & Business Excellence	Manufacturing		To propose and develop a new set of constructs to assess LSSA and understand how it will Influence the Lean Six Sigma Implementation in the manufacturing industries in India.	Lean Six Sigma Awareness	Impact of Lean Six Sigma, Acceptance towards Lean Six Sigma	top management commitment, Lean Six Sigma Implementation			SEM	India
M. N. Ibrahim, M. S. Ibrahim, A. Mohd-Din, K.Abdul-Hamid, R. M. Yunus, M. R. Yahya, The 2nd International Building Control Conference 2011	Heritage building	Survey	examines the perspectives of different parties involved in fire management/risks/protection system of heritage building	Risk managment	Passive Protection System, Active Protection System, Fire Management, Bulding characteristic	Fire risk Management			AHP	Malaysia

Authors	Domain	Method	Objective / Focus	Model Theory / Concept	Independent Variable	Dependent Variable	Mediating Variable	Moderating Variable	Tools & Technique	Region
Kazaras, K., Kirytopoulos, K., & Rentizelas, A. (2012). Introducing the STAMP method in road tunnel safety assessment. Safety science, 50(9), 1806-1817.	Tunnel	STAMP based technique	To establish a proactive safety strategy and evaluating the overall safety of critical infrastructures		Human errors and behavior during accident conditions, Lack of data and uncertainties Organizational factors and safety culture	safety				Greece
Hanan Altabbakh, Mohammad A. AlKazimi, Susan Murray and Katie Grantham, Identifying a Need for Undergraduate Engineering Students, Professional Safety, 2015, 38-41.	Education building	Survey	To identify safety awareness among undergraduate engineering students		Safety Training, Safety Knowledge, Safety Attitude, Safety Consciousness	Safety Awareness				USA

In the nutshell, the comparison of all related works and the summarization of related works in awareness model. Most of student focusing on software security rather software security awareness. Therefore, this study founded that software security awareness as gap based on the finding of literature review. Therefore, this study take consideration with three importance factors based on the awareness of software security.

IV. Related model of awareness in software security

Software security is an important aspect in the IT industry with the immense vulnerabilities affecting different projects and in this sense, smart city implementation. Hence why, creating effective security awareness and training programs is necessary to create security awareness. According to Banerjee and Pandey (2010), several academic bodies and universities have already designed and developed programs for creating security awareness programs, but none totally and sufficiently addressed the software security issues that focused on awareness. Hence why, after conducting a literature review that highlighted the value of security awareness through the aid of current published work for establishing more secure software, Banerjee and Pandey (2010) suggested the areas in the figure below that could create awareness among various software engineering teams shown in Figure 2.

Figure 2: Techniques of Software Security Awareness (Banerjee & Pandey 2010, p.4)

As enumerated, the suggested awareness areas in training and education, campaign, interview and questionnaire, survey, industry/ academia interaction, test and experiments, games and simulations, industry/ academia tools, online community, and media and related areas. These could be suggested as the curriculum needed for security awareness programs, which could also be reflected on the suggestions for future research of Banerjee and Pandey (2010). Future research work should include sound training program that covers current security incidents, employees' management, customer and investor concerns, and regulatory issues with definition of training, target audience identification, delivery frequency and support from management (cf. Olzak, 2006).

Bogolea and Wijekumar (2017) surveyed IT professionals with the intent of acquiring information about their needs for employees with security training and areas of security considered of highest concern. Based on the themes extracted by the researchers, information security awareness was found under the curriculum topic "Information Security Fundamentals," which contained the following contents in Table 5:

Table 5: Content of Information security

Curriculum	**Content**
Information Security Fundamentals	➢ Information Security concepts like confidentiality, integrity, availability, authentication, auditing, etc. ➢ Information Security awareness ➢ Threats and vulnerabilities like viruses and other malicious codes ➢ - Legislation and industry standards

On a relevant note, Security Innovation Europe (2018) has highlighted eight essential components for an effective security awareness curriculum for employees, while stressing that this is the first step in improving security. In order to ensure that every employee understands the need for security, the eight (8) crucial components, as shown in the figure below, should be rolled into an awareness program, which taps on the biggest threats affecting the organization.

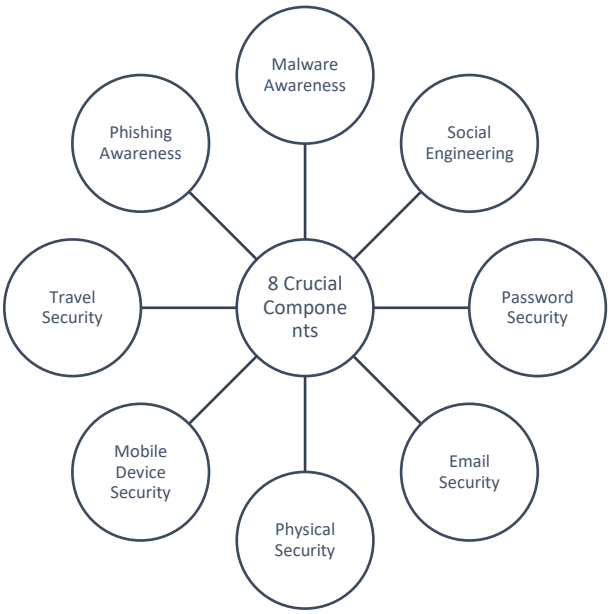

Figure 3: Essential components for an effective security awareness curriculum for employees according to Security Innovation Europe (2018)

Security Innovation Europe (2018) has elaborated each of the suggested eight important components for effective security awareness curriculum for employees, as detailed in the follows:

1. Malware awareness – Malwares or malicious software has been considered as a huge problem in organizations, as more and more employees are installing unapproved and unauthorized software in both work and home networks. In order to reduce threats caused by malwares, employees must be taught to identify common types of malware.
2. Social engineering – Techniques of psychological manipulation can make social engineering highly inevitable—considering how it can massively affect security with how regularly compromised login details and secure information are, through unsolicited calls, emails and in-person visits. Such issue can be mitigated with raising awareness for common social engineering strategies and educating employees about the Social System for security awareness.
3. Password security – Passwords are considered as one of the largest and most easily remedied security problems in huge organizations. As known, passwords are utilized for securing applications and devices. It serves as guard for unauthorized access to data. It is essential to raise awareness about the best practices for password security as creating weak, insecure and reused passwords can cause massive security issues.
4. Email security – Emails can also serve as huge source for possible security vulnerabilities, through malicious attachments, phishing for sensitive data or disguised malware. Raising awareness on the common threats in emails educates employees to identify common threats in emails and for them to be taught how to flag and dispose malicious emails.
5. Physical security – Several security issues can occur in an organization's computer network due to physical vulnerabilities. Employees should therefore be educated about the threats of data theft from mobile devices, unlocked drawers and desks, and even post it notes.
6. Mobile device security – Mobile working has been an essential trend due to smartphones, tablets and laptops. This allowed personal devices to be utilized for access and data storage. In order to protect information from los and theft, it is important for organizations to create and promote codified Bring Your Own Device policy for remote working.
7. Travel security – Working remotely has combined threats from mobile devices and physical security breaches. Therefore, travel security has grown problematic than before. Commonly, organizations consider security to be something at the front door of their premises, but the reality of journeying to work can really become serious

source of security issues and problems, such as theft and lost devices. Therefore, employees should be educated about the risks of remote working and must understand when mobile devices should be secured.

8. Phishing awareness – Phishing is regarded as a social engineering variant that utilizes misleading emails and webpages for extracting sensitive data. To tighten security on email clients and web browsers, employees should be educated about the threats and common hallmarks of phishing attacks.

Moreover, security challenges are considered as a crucial determinant of the success of smart services projects' implementation. In the study of Marquardt (2017), the authors noted that security and data privacy are considered as the major challenges in the development and provision of smart services. According to Cui, et al (2018), due to the several smart systems that have already been implemented, security and privacy issues have become a major challenge. Part of this security challenge includes deficits in technology and data analytics, lack of standards and interoperability and cybersecurity threats among others (Marquardt, 2017; Cui, et al, 2018). Therefore, in order to overcome this problem, smart government needed considered software security awareness to success developing smart cities in United Arab Emirates.

V. Conclusion

An analysis of methods and model of awareness model has been conducted. A list of existing works related to awareness model has been presented in Table 4. Based on the analysis of existing works, work that analyzes awareness factors and attention to use software security awareness model in smart cities is yet to be conducted and most of previous work did not consider awareness in software security. Moreover, most of the works in awareness model focus on the industry services. There are model and method involved in various domains, which are manufacturing and automotive. The finding indicates that there is no outstanding work of awareness model of using software security in smart citie of Smart government United Arab Emirates. For future work, we plan to develop a new conceptual framework for software security model for Smart Cities in UAE.

VI. Acknowledgement

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

VII. 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]. 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

[4]. 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>

[5]. 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

[6]. 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

[7]. Banerjee, C. and Pandey, S. K. (2010). Research on software security awareness: problems and prospects. ACM SIGSOFT Software Engineering Notes, 35(5), 1-5

[8]. 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

[9]. Bernardo, M. R. M. (2017). Smart City Governance: From E-Government to Smart Governance. In: Entrepreneurial Development and Innovation Within Smart Cities. IGI Global

[10]. 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.

[11]. 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.
[12]. Bogolea, B. & Wijekumar, K. (2017). Information Security Curriculum Creation: A Case Study, pp.55-65.
[13]. Caird, S. P. and Hallett, S. H. (2019). Towards evaluation design for smart city development. Journal of Urban Design, 24(2), 188-209
[14]. 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
[15]. 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
[16]. Chua, W. F. (1986). Radical Developments in Accounting Thought. The Accounting Review, 66(4), 601-632
[17]. 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.
[18]. Cohen, L., Manion, L. and Morrison, K. (2000). Research Methods in Education. London: Routledge
[19]. Comte, A. (2009). The Positive Philosophy of Auguste Comte, Vol. 1. New York: Cosimo
[20]. 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>
[21]. 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
[22]. Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2008). Management Research, Third Edition. London: SAGE Publications
[23]. Eremia, M., Toma, L. and Sanduleac, M. (2017). The Smart City Concept in the 21st Century. Proceedia Engineering, 181, 12-19
[24]. Flynn, M., Rao, A. K. and Gashi, D. S. (2018). Smart Cities Funding and Financing in Developing Economies. Deloitte
[25]. 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
[26]. Gray, D. E. (2004). Doing Research in the Real World. London: SAGE Publications.
[27]. 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
[28]. Hancock, B. (1998). An Introduction to Qualitative Research. Nottingham. UK: Trent Focus Group, Division of General Practice, University of Nottingham.
[29]. Hancock, B., Ockleford, E. and Windridge, K. (2009). An Introduction to Qualitative Research. The NIHR RDS for the East Midlands / Yorkshire & the Humber (Leicester)
[30]. Harvey-Jordan, S., & Long, S. (2001). The process and the pitfalls of semi-structured interviews. Community Practitioner, 74(6), 219-221.
[31]. Howard, M. & Lipner, S. (2006). The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software. Redmond, WA: Microsoft Press.
[32]. 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
[33]. 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
[34]. Keegan, S. (2009). Qualitative Research: Good decision Making Through Understanding People, Culture and Markets. London: Kogan Page Ltd.
[35]. 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>
[36]. 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
[37]. 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.
[38]. 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.

[39]. 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

[40]. 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.

[41]. Marquardt, K. (2017). Smart Services – Characteristics, Challenges, Opportunities and Business Models. 11th International Conference on Business Excellence 2017, At Bucharest

[42]. Matrooshi, S. R. O. K. (2016). The Challenges of Developing Smart Services Projects in the United Arab Emirates. Thesis. The British University in Dubai

[43]. 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.

[44]. 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

[45]. 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

[46]. Mutiara, D., Yuniarti, S. and Pratama, B. (2018). Smart Governance for Smart City. Earth and Environmental Science, 126, 1-11

[47]. 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.

[48]. New, J., Castro, D. and Beckwith, M. (2017). How National Governments Can Help Smart Cities Succeed. Center for Data Innovation

[49]. Olzak, T. (2006). Strengthen Security with an Effective Security Awareness Program. Retrieved from http://adventuresinsecurity.com/ Papers/Build_a_Security_Awareness_Program.pdf

[50]. 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

[51]. 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

[52]. 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.

[53]. Plas, J. M., Kvale, S. and Kvale, S. A. (1996). InterViews: An Introduction to Qualitative Research Interviewing. Sage Publications

[54]. 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.

[55]. 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.

[56]. Security Innovation Europe (2018). Effective security awareness curriculum. Retrieved from < https://www.securityinnovationeurope.com/blog/page/effective-security-Awareness-Curriculum>

[57]. 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.

[58]. Staller, K. M. (2010). Qualitative Research. In: Encyclopedia of Research Design, Vol. 3, Neil J. Salkind (Ed). Thousand Oaks, CA: Sage

[59]. Sujata, J., Saksham, S., Tanvi, G. and Shreya. (2016). Developing Smart Cities: An Integrated Framework. Procedia Computer Science, 93, 902-909

[60]. 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.