2017

Security readiness evaluation framework for Tonga e-government initiatives

Raymond Lutui
Auckland University of Technology

Semisi Hopoi
Christ's University in Pacific

Siaosi Maeakafa
Christ's University in Pacific

DOI: 10.4225/75/5a84f2bd95b4a
Lutui, R., Hopoi, S. & Maeakafa, S. (2017). Security readiness evaluation framework for Tonga e-government initiatives. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.14-24).

SECURITY READINESS EVALUATION FRAMEWORK FOR TONGA E-GOVERNMENT INITIATIVES

Raymond Lutui[1], Semisi Hopoi[2], Siaosi Maeakafa[3]
[1]School of Engineering, Computer & Mathematical Sciences, Auckland University of Technology
Auckland, New Zealand
[2, 3]School of Computer Science, Christ's University in Pacific, Nuku'alofa, Tonga
rlutui@aut.ac.nz, halahalalahi@gmail.com, gmaeakafa@yahoo.com

Abstract

The rapid expansion of the Information and Communication Technologies (ICTs) in the Pacific have reached the Kingdom of Tonga. The submarine fibre-optic cable which connects Tonga to Fiji and onward to a hub in Sydney went live 2013. Now the people of Tonga experience the high-speed impact of digital communication, fast international access, and social changes such as the government is implementing a digital society through e-government services. This study focuses on identifying the factors that will later become a vulnerability and a risk to the security of Tonga government e-government initiatives. Data was collected through interviews with three government officials, document analysis, and critical reflection on the theory context. Consequently, a security-readiness evaluation framework has been designed from the data analysis to inform the e-government initiatives. This study contributes a security-readiness evaluation framework for use in developing countries to guide the implementation of e-government initiatives.

Keywords: E-Government, information security, information systems, cyber security, security threats, security risks, socio-technical

INTRODUCTION

The immense growth in the communication technologies' domain over the last two decades, have changed the way we live our lives and conduct day to day businesses. Information and Communication Technology (ICT) is one of the most vital traits of every new development (Alshehri & Drew, 2010, p.35). This trend of technological advancements has reached the Kingdom of Tonga. In 2010, Tonga Communications Corporation (TCC) – the country's leading provider of complete end-to-end telephony and Internet services – launched the new mobile-broadband-enabled GSM to replace the previous macro-GSM network (Grealish, 2010, P.1). On the 21st August 2013, the first submarine cable (fibre optic) that connects Tonga to the outside world went live (Matangi Tonga, 2013, P.1).

The Kingdom of Tonga is one of the developing countries in the South Pacific with a population of just over 107 thousand. In 2009, the Government of Tonga has identified Information and Communication Technologies (ICT) as an engine for growth in a national ICT vision and strategy. This focuses on Education, Health, Environment Sustainability, and Industry Growth. The National ICT policy for Tonga consists of six main components - Provision of ICT in Homes and Communities, Education and Skill Development, E-Government, Industry Growth and Economic Development, An enabling technical infrastructure and the ICT related legislation (Ma'u, 2015, p.1). The rapid growth of ICT technologies in Tonga is evident in the literature. In 2010, the Tonga Communications Corporation (TCC) – the country's leading provider of complete end-to-end telephony and Internet services – launched the new mobile-broadband-enabled GSM to replace the previous macro-GSM network. Before the introduction of the fibre optic cable, only 20% subscribers across the country for Internet. At the time of writing this paper, over 75% of the country subscribes for an Internet connection.

The Government of Tonga is now talking about implementing e-Government services as part of the National ICT policy for Tonga. The aim is to generate a more efficient way for its government to deliver information and services to its citizens and the business community over the Internet (Cullen & Hassall, 2017, P.4). The completion of the fibre optic cable project, boosted the experience of the people of Tonga in cyber space. The e-government initiative is in its planning stage but need to consider all factors that might affect its successful completion. The aim of this study is to develop a framework to evaluate the readiness of Tonga e-government with regards to cyber security.

According to Grönlund and Horan (2005), the e-government field appeared in the late 1990s. E-government is also known by other names such as e-Gov, Electronic Government, Digital Government, Electronic Governance, and so on (p.39). E-government is defined as, the government owned or operated systems of information and communication technologies that transform relations with citizens, the private sector and/or other government agencies so as to promote citizens' empowerment, improve service delivery, strengthen accountability, increase transparency, or improve government efficiency (Ndou, 2004, p.18). Ndou (2004) rightly argued that, e-governance is more than just a government website. The strategic objective is to support and simplify governance for government, citizens and businesses. The use of ICTs can connect all three parties and provide support for processes and activities (p.18).

The potential of what ICT technologies can provide towards public administration and governance procedures is apparent. However, technology trends such as mobile computing, social media, etc., have introduced new challenges in e-government service design and implementation (Layne & Lee, 2001, p.122). On the other hand, challenges introduced by e-government to information security and privacy is significant. Taking into account the importance and criticality of systems involved in a comprehensive e-government services framework such as e-health, e-tax services, e-education, e-ID, e-procurement, etc., a security breach is immense due to the amount of personal information collected (Layne & Lee, 2001, p.125). Figure 1 shows the security priorities of e-government.

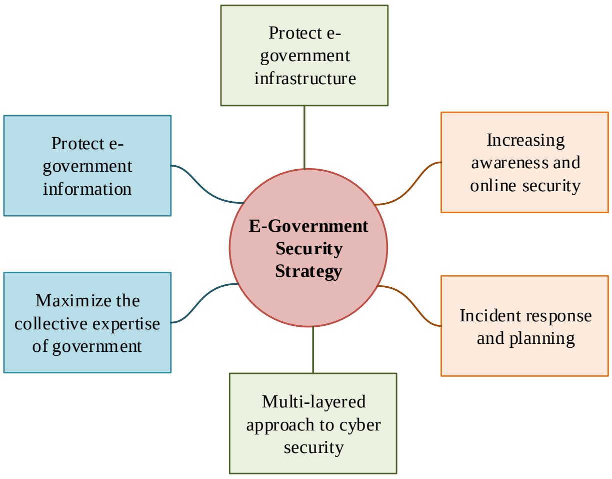
Protect e-government infrastructure
Protect e-government information
Increasing awareness and online security
E-Government Security Strategy
Maximize the collective expertise of government
Incident response and planning
Multi-layered approach to cyber security

Figure 1: E-Government security priorities

As a result, with e-government, information security issues are becoming ever more prominent. An attack on e-government information system such as hacker attacks, malicious software intrusions, computer crimes and privacy breaches constitute great threats to information security. In addition, developments in both science and technology have posed new challenges to information security (Zhang et al., 2015, p.3). This study can contribute to both theory development for security system integration and practical guidance for operational system that protect information. Taking a socio-technical approach to e-government will show that the balance is between the system and the users. This has to be sensitively and economically managed in order to gain the optimal performance.

The biggest threat to information security today is social engineering and the socio-technical interface between systems and its users. Theoretically, most information system can be strongly protected from attacks but the vulnerability remains of human factors who either by mistake, by trickery, or by intention, knowingly or unknowingly compromise information security (Algarni, et al., 2013, p.510). The literature suggests that it is possible to design e-governance system that interlocks management systems and operational control systems. However, such relationship is dynamic along the lines of interaction so that concepts such as defence in depth are no longer relevant. The security of an information system has both technical and social dimensions.

SOCIO-TECHNICAL APPROACH

The increasing availability of ICT technologies quantified the complexity of socio-technical systems (Vespignani, 2012, p.32). Sociotechnical system (STS) is defined as an approach to complex organizational work design that recognizes the interaction between people and technology. The term also refers to the interaction between society's complex infrastructures and human behaviour (Salnitri, Paja, & Giorgini, 2014, p.50). Therefore, STSs are complex systems where social (human and organizational) and technical components interact with each other to achieve common objectives. For instance, healthcare systems, smart cities, air traffic management, etc. Based on the statement, e-government systems are complex systems and only make sense to employ socio-technical approach in designing such a system. This study is a social technical system design study which is designed to deal with the governance, management and control of security risk.

In a smart city, citizens will be constantly accessing e-government services such as tax-payment, e-visa application, e-electricity, etc. The amount of information exchanged in such system is substantial, and such information is sensitive and should be secured. In the modern holistic view, the sociotechnical system (STS) is the whole system, not one of two side-by-side systems (Whitworth, 2009, p.395). For instance, a pilot plus a plane are two side-by-side systems with different needs, one mechanical (plane) and one human (pilot). Human Computer Interaction (HCI) suggests these systems should interact positively to succeed (Issa & Isaias, 2015, p.20). However, the plane and the pilot can be seen as a single system. On the mechanical level, the body of the plane and the body of the pilot both have weight, volume, and so forth. However, the pilot adds the human thought level which is above the plane's mechanical level. This allows the plane and pilot system to strategize and analyse.

The socio-technical concept that will be developed changes the priorities, for example, if a social system sits next to a technical one, it is usually secondary. Then, when a social system sits above a technical one, it guides the entire system and that is the primary factor in system performance (Miller, 2004, p.31). Online communities such as e-government, are social-technical systems (STS), built upon social requirements as well as technical ones like bandwidth. As technical problems are increasingly solved, social problems like spam rises. If software can do almost anything in cyberspace, there is still the challenge of what should it do? (Whitworth, de Moor, & Liu, 2006, p.249).

Social Element of Information Security

Securing information assets whether in storage or transmitting around the system is critical and challenging for businesses who rely on ICT to support day to day processes (Dhillon & Backhouse, 2000, p.125). However, advancements of information security technologies do not always guarantee security of information assets. The human factors of information security will always be a challenge and an issue in terms of managing of security (Siponen et al., 2014, p.217). As a result, a security framework is required to combine systems, operation, and internal controls to ensure confidentiality, integrity, availability of the critical information assets. Due to the seriousness of threats of unauthorized access over the Internet, effective information security management is one major concerns. A malicious insider is defined as a current or former employee, contractor, or business partner who - has or had authorized access to an organization's network, system, or data, has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems (Silowash et al., 2012, p.9).

Security mechanisms such as firewalls, intrusion detection systems (IDS), and electronic access systems to enter the building or rooms. These are implemented particularly as a protection against external threats. However, that still does not address the issues of insider threats. Insiders not only aware of their organization's policies, procedures, and technology but, they also aware of the known vulnerabilities in the system. The ISACA's Cybersecurity Snapshots of the issues facing organizations revealed that, the top three cyber threat are social engineering, insider threats and advanced persistent threats. The 2017 Cyber Security Survey reported that 65% of the IT security professional respondents are not confident in their organizations security posture (Meyer, 2017, p.2). According to (CERT, 2011), the threat of attack from insiders is real and substantial. Another study conducted by (CSO Magazine, 2011, p.1) explained that 46% of the respondents thought that damage caused by insider attacks was more severe than damage from outsider attacks. The study found that the most common insider crimes were - unauthorized access to or use of corporate information; unintentional exposure of private or sensitive data; viruses, worms, or other malicious code; theft of intellectual property (IP).

(Silowash et al., 2012, p.2) discussed that, insider threats are influenced by a combination of technical, behavioural, and organizational issues and must be addressed by policies, procedures, and technologies. (Silowash et al., 2012, p.9) also added that their current analysis recognizes that - intellectual property (IP) theft, IT sabotage, fraud, espionage, and accidental insider threats seems to be the unique patterns of insider threat behaviour. Siponen et al., (2014) pointed out that, the key threat to information security comes from employees who do not comply with information security policies (p.220).

Technical Element of Information Security

In von Solms (2010), the author discussed the five waves of information security. The first wave is technical wave, second wave is management wave, third wave is institutional wave, fourth wave is information security governance wave, and the fifth wave is the cybersecurity wave (p.2). In the era of the technical wave, Information

Security main concern was a form of Identification and Authentication for logging onto the mainframe system, and Logical Access Control. Most of these functions were handled by technical people.

Whitman and Mattord (2016) explained that, there are six critical components of information system, the hardware, software, networks, people, procedures, and data enable information to be input, processed, output, and stored (p.114). Each of these IS components has its own strengths, weaknesses, characteristics and security requirements. The hardware component is dealing with technical and physical technology that is responsible executing, storing and transmitting of the data. Settanni et al., (2017) stated that, today's information systems are increasingly complex. Their interconnected nature exposes them to advanced cyber threats (p.167). Anderson and Fuloria (2010) pointed out that, a failure of critical infrastructure can cause significant damage within a short period of time (p.55). There are a number of various threats to critical infrastructure such as the most obvious, natural disasters such as flooding, fire, equipment malfunction or also human error. However, recently, targeted attacks by hackers on the information system infrastructures has become significant (Miller & Rowe, 2012, p.51).

There is a lot involved in physical/technical elements of information security. However, physical/technical security system such as a 24x7 security guard and surveillance cameras. Access to areas where confidential work is done usually require electronic access cards or biometric access system. Security cameras is in place and uses of personal memory devices or CD/DVD ROMs are not allowed. All network/Information System traffics are configured to go through a firewall and a proxy server so web access and activities can be monitored and controlled. Access rights are controlled so no one can have the rights to execute .exe files. All files are redirected to store on the server not locally so they can be backed up regularly and stored offsite.

DESIGN OF THE STUDY

Exploratory research, on the other hand, is employed in this type of study as it allows the researcher to gain a deeper understanding of an issue or problem. Jebb et al. (2017) describe that, exploratory perspective is designed ready to find patterns that are different than expected. Such patterns may provide theoretical insights or provide information to guide further analyses (p.266). As a result, Exploratory research is the chosen methodology for this study.

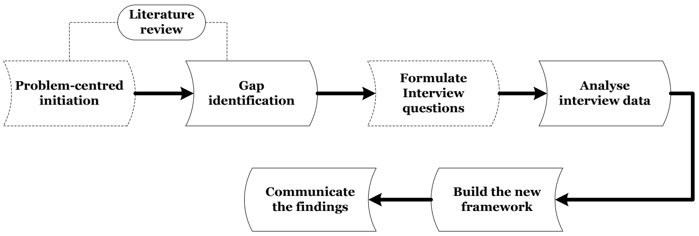

Figure 2: Design of the study

The study is designed to first identify the problem – the gap for this study based on the literature survey. The next task is to define the problem and extract its significance. This involves analysing the existing and relevant literature; identify the problem, interview experts in the field. This presents an opportunity to employ a gap analysis strategy by completing a component-by-component analysis. Therefore, influencing how the interview questions should be designed to create awareness of factors that will affect the security readiness of Tonga e-government initiative. The next stage is designed to deal with the formulation of the interview questions for data collection. The next stage deals with data analysis, in this phase, the factors that will affect the security readiness of the Tonga e-government will be identified. The data gathered from this phase will be used to construct the security evaluation framework for the Tonga e-government initiative. The final phase is designed to allow the researcher to employ various scholarly electronic databases to communicate the outcome of the study. This communication might include the problem and its importance, the artefact and its effectiveness to other researchers and practitioners in the field including the Government of Tonga. It is also suggested that researchers should conclude the study with communicating the implications of the result for the practical field.

Data Analysis and Discussions

An interview was conducted with three senior government officials of the Tonga government. At the moment, there only two government ministries that was formed to work on the Tonga e-government initiative together with a consultant from the Asian Development Bank (ADB) based on the National ICT policy for Tonga. This is why this study only interview the three top officials that are working on the Tonga e-government. The three officials are the consultant from the ADB, the CEO of Tonga Computer Emergency Response Team (CERT) and the Senior

Engineer from the Ministry of Meteorology, Energy, Information, Disaster Management, Climate Change and Communications (MEIDECC). Table 1 summaries the answers received and has been categorised into four categories but grouped into only two main groups.

Table 1: Security requirement categories interview data

Questions	Technological	Policies & Regulations
• What are the benefits of employing ICT? • What are the challenges faces by the Government in implementing ICT? • How well are e-Government initiatives aligned with Tonga frameworks and requirement? • Who is driving these initiatives? • How are they going to be funded?	• Access to information • Decision making • Centralized DataBase • Share Information • Easy communication • Build each Ministry's ICT capacity • Unsecured software application • Unsecured ICT infrastructure • Inexperience staffs • Unskilled IT staffs	• Lack of proper tools for the job • Lack of funding • Lack of inter-ministry communication • Lack of top management support • Too much politics • Dependent on overseas donations • Out-of-date computer crimes act

The next phase is to prepare and get the data organized. The next phase is designed to provide a description of the case considered. During this phase, data coding is done also, a number of questions is asked such as, what is this incident about? what category does this incident indicate? what property of what category does this incident define? what is the 'main concern' of the participants? The coding of the data was based on their properties and security requirements. Properties considered in this study are conditions, causes, consequences, hierarchies and contexts. However, this study further grouped these categories into two groups as it shown in table 1. The purpose is not only to summarize the interview data but to identify their inter-relationships and establish how they help to explain the phenomenon under study.

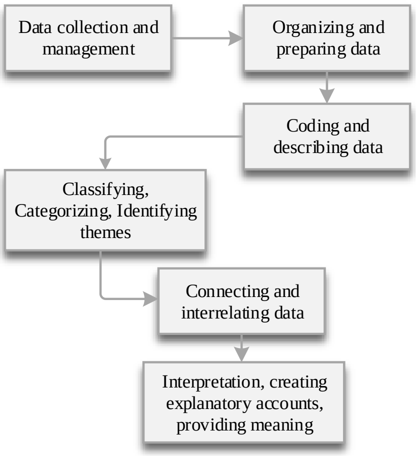
Data collection and management
Organizing and preparing data
Coding and describing data
Classifying, Categorizing, Identifying themes
Connecting and interrelating data
Interpretation, creating explanatory accounts, providing meaning

Figure 2: Data analysis technique

The final phase is designed to allow for interpretation, developing explanations and provide meaning for the data. As mentioned earlier, this study is taking a socio-technical approach to cyber security of e-government, more specifically, Tonga e-government. Looking at the interaction between social and technical dimensions of modern life as dynamic, constantly changing that both emerge from and shape modern society. As the technological age advanced, however, it presented an ever-growing array of new issues and unknowns. In response, practitioners began to focus on more specific areas for action, and most researchers began to select more narrowly defined subjects for study. The security needs are expressed through the processes.

SECURITY READINESS EVALUATION FRAMEWORK

Based on the coding done of the interview data, following are the security challenges to Tonga e-government can be identified. However, due to the complexity of e-government systems, these security challenges might affect implementation and management. According to Evans (2011), by 2020 there will be over 50 billion connected objects against a population of 7 billion. An object can be anything embedded with computation, storage and communication capabilities with different capacities (sensor, actuator, mobile phone, desktop, laptop, printer, car, fridge, oven, etc.) (p.7). Therefore, security in such environment is paramount. The main objectives of e-government initiatives are to provide one-stop quality public services and value-added information to citizens and businesses. At the same time, to enable government agencies to work together and achieve internal efficiency and effectiveness of operations (Lee et al., 2005, p.99).

The UN survey reported that efforts are being made to ensure privacy and security of personal data yet challenges remain. Some related to the technical difficulties associated with ensuring interoperability of systems. However, proliferation of technologies makes it difficult to provide integrated services such as e-health, etc. Major security services required for e-government consists of three aspects that should be considered:

- **Confidentiality:** refers to protection of information from unauthorized disclosure e.g. to the press or to release through improper disposal techniques, or to those who are not entitled to have the same.
- **Integrity:** is about protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.
- **Availability:** is to ensure that the information is available when it is required.

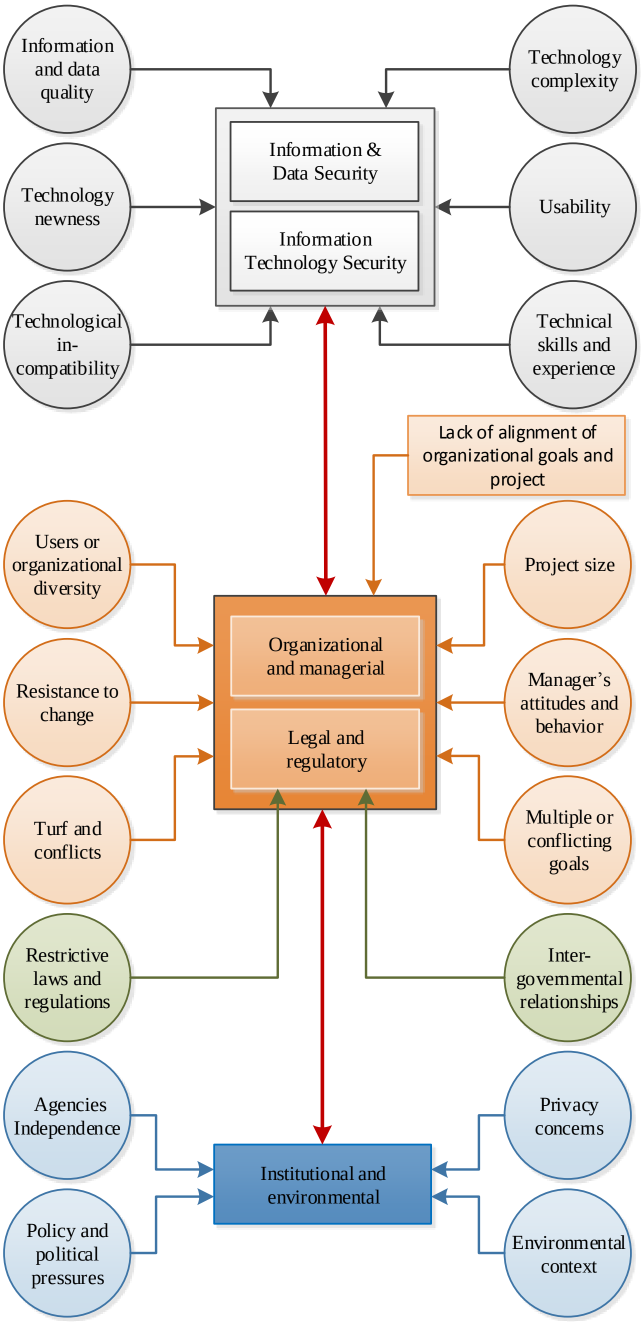
Information and data quality
Technology complexity
Information & Data Security
Technology newness
Usability
Information Technology Security
Technological in-compatibility
Technical skills and experience
Lack of alignment of organizational goals and project
Users or organizational diversity
Project size
Organizational and managerial
Resistance to change
Manager's attitudes and behavior
Legal and regulatory
Turf and conflicts
Multiple or conflicting goals
Restrictive laws and regulations
Inter-governmental relationships
Agencies Independence
Privacy concerns
Institutional and environmental
Policy and political pressures
Environmental context

Figure 4: Security e-readiness evaluation framework.

Information and Data Security

E-government initiatives are goals set up by governments and accomplished through the use of ICTs. E-government initiatives are focused on capturing, management, use, dissemination, and sharing, of information. A number of the challenges relate to the information at the core of E-government initiatives. Researchers in the e-government domain principally focused on the issues relating to quality and accuracy of the data. However, legal experts expressed their concerns regarding the fact that every data processing duplicates the risk of abuse (intended or not). On the other hand, poor data quality increases operational cost because time and other resources are spent detecting and correcting errors. Information is power and organizations tend to be sensitive about giving out information as it reflects on the quality of their operations. As a result, information has to be used differently and its management in order to satisfy the digital requirements. System usability and ease of use are an important factor to consider when designing E-government initiatives. Complexity and newness of technology are also constraints that can potentially affect the results. The lack of relevant technical skills within the ministries has been found to be an important factor as well as the shortages of qualified technical personnel.

Organizational and Managerial

The size of the implementation and the diversity of users and organizations involved are two of the main challenges for E-government initiatives. There are at least two other problems related to the goals and objectives of the initiative. First is the lack of alignment between organizational goals and the E-government project. This alignment may be understood as a certain type of balance that needs to be in place to achieve one or more goals. Contextual factors are often addressed in information systems (IS) research as situational, organizational, environmental, task, and technology characteristics with influence for the outcome of an E-government project.

E-government initiatives are required to be value-driven and not technology driven. The promised benefits of E-government cannot be based on digitizing information and putting it on the web alone. Technology needs to be fully realized and the transformation brought about to better serve the citizens. E-government is to facilitate an information society that can influence every aspect of daily life. Yet, more detached observers maintain that there is no post-industrial society therefore, individual interests and associated behaviours lead to internal conflicts about change and resistance to innovation is such as E-government.

Legal and Regulatory

Government ministries operate according to a specific and formal sets of rules. Li (2003) pointed out that, e-government is not a technical issue, but an organizational issue (p.45). As a result, to successfully implement e-government principles and functions, will require a new set of rules, policies, and laws. There will also be changes to satisfy the requirements for electronic activities such as electronic archiving, signatures, transmission of information, data protection, computer crime, intellectual property rights and copyright issues and so on. Dealing with e-government means signing a contract or a digital agreement, which has to be protected and recognized by a formalized law (Hwang et al., 2004, p.10). In Tonga, e-business and e-government laws are not yet available.

Institutional and environmental challenges

The availability of resources is an economic challenge associated with emerging technologies that is a great challenge for developing countries. Obstacles with funding, regulations, and patents that can derail technology development and adoption (Woodson, 2016, p.1410). However, in this environment, institutions are not only laws and regulations, but also norms, actions, or behaviours that people accept as good or take for granted. On the other hand, deployment of security measures can lead in to an intrusion on users' privacy. Privacy and related security issues are challenges that must be adequately addressed in E-government IT initiatives (Arroyo et al., 2015, p.455). In this digital age, it is not possible to imagine conducting day to day work without the use of technology.

External pressures such as policy agendas and politics may affect the results of IT initiatives. The discussion highlights the range of complex and various challenges public managers must face as they work in the e-government area (Walker, 2015, p.297). Success is not only about choosing the right technology, but also managing organizational capabilities, regulatory constraints, and environmental pressures. For E-government managers to be successful in their initiatives they must be aware of these challenges and use appropriate strategies to overcome the institutional and environmental challenges.

Digital Divide

The digital divide refers to the gap in opportunity between those who have access to the Internet and those who do not. Those who do not have access to the Internet will be unable to benefit from e-government services. Digital Divide is a very serious matter in Tonga, not all citizens currently have equal access to computers, it can an issue of affordability or lack of necessary skills (Lu, 2001, p.1). Government should look providing Internet-enabled computers in schools and public libraries. Yet, few types of challenges that government may face are-affordability, elderly, language barrier, and the inexperienced or computer illiterate or not so well educated (Hassani, 2006, p.250). Government should provide basic skills training to both its employees and citizens in order to let them participate in e-government development applications.

CONCLUSION

The result of the literature survey highlighted the fact E-government is a complex system and Socio-technical system (STS) is defined as an approach to complex organizational work design that recognizes the interaction between people and technology. As a result, this study decided to take a Socio-Technical approach to e-government security because, in the modern holistic view, the sociotechnical system (STS) is the whole system, not one of two side-by-side systems that is – social and technical. Human Computer Interaction (HCI) suggests these systems should interact positively to succeed.

Interview was used as the method of data collection. The growth of ICT technologies is very fast however, the country is very small and lack of expert personnel in the field seems a real issue. The interview data was collected from three experts in Tonga that are currently involve with the e-government initiative. The purpose of the study is to identify the factors that may become a risk and a vulnerability of Tonga e-government services. E-government presents several technical, economic and social challenges that will surface as the E-government development moves forward. Looking at various reasons to why security-readiness is so important to both governmental and non-governmental organizations, the ease of using these measures is most prominent. Having an easily quantifiable set of indicators is vital. This will provide the government of Tonga with an overview of their situations. It can be also used as a basis for comparison and future planning. This advantage arises from the fact that security-readiness measures have the ability to summarize a broad set of characteristics of the Kingdom of Tonga.

There are a number of existing security-readiness evaluation frameworks with various objectives, methodologies and results. However, there is no one fits all evaluation framework yet, and this study has contributed a security-readiness framework that is both relevant and practical for implementation in a developing country.

REFERENCES

Algarni, A., Xu, Y., Taizan, C., & Yu-Chu, T. (2013). Social engineering in social networking sites: Affect-based model, *Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 508-515). UK: IEEE.

Alshehri, M., & Drew, S. (2010). E-Government Fundamentals, *Proceedings of the IADIS International Conference ICT, Society and Human Beings* (pp. 34-42). Freiburg: MCCSIS.

Anderson, R., & Fuloria, S. (2010). Security Economics and Critical National Infrastructure. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 55-66). Boston: Springer.

Arroyo, D., Diaz, J., & Gayoso, V. (2015). On the Difficult Tradeoff Between Security and Privacy: Challenges for the Management of Digital Identities. In Á. Herrero, B. Baruque, J. Sedano, H. Quintián, & E. Corchado (Eds.), *International Joint Conference: CISIS'15 and ICEUTE'15* (pp. 455-462). Cham: Springer.

Basu, S. (2004). E- government and developing countries: an overview. *International Review of Law, Computers & Technology, 18*(1), 109-132.

Cullen, R., & Hassall, G. (2017). E-Government in Pacific Island Countries. In R. Cullen & G. Hassall (Eds.), *Achieving Sustainable E-Government in Pacific Island States* (pp. 3-32). Cham: Springer

DeLisi, P. S. (1990). Lessons from the steel axe: culture, technology, and organizational change. *MIT Sloan Management Review, 32*(1), 83.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Commun. ACM, 43*(7), 125-128.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper, 1*(2011), 1-11.

Grealish, A. (2010). *Altobridge wireless network goes live in tonga*. Retrieved July 25, 2017, from https://www.realwire.com/releases/Altobridge-Wireless-Network-goes-Live-in-Tonga

Grimsley, M., & Meehan, A. (2007). e-Government information systems: Evaluation-led design for public value and client trust [journal article]. *European Journal of Information Systems, 16*(2), 134-148.

Grönlund, Å., & Horan, T. A. (2005). Introducing e-gov: history, definitions, and issues. *Communications of the association for information systems, 15*(1), 39.

Hassani, S. N. (2006). Locating digital divides at home, work, and everywhere else. *Poetics, 34*(4–5), 250-272.

Hwang, M.-S., Li, C.-T., Shen, J.-J., & Chu, Y.-P. (2004). Challenges in e-government and security of information. *Information & Security, 15*(1), 9-20.

Issa, T., & Isaias, P. (2015). Usability and Human Computer Interaction (HCI). In *Sustainable Design: HCI, Usability and Environmental Concerns* (pp. 19-36). London: Springer.

Jebb, A. T., Parrigon, S., & Woo, S. E. (2017). Exploratory data analysis as a foundation of inductive research. *Human Resource Management Review, 27*(2), 265-276.

Jones, S., Hackney, R., & Irani, Z. (2007). Towards e-government transformation: conceptualising "citizen engagement" A research note. *Transforming Government: People, Process and Policy, 1*(2), 145-152.

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2), 122-136.

Lee, S. M., Tan, X., & Trimi, S. (2005). Current practices of leading e-government countries. *Commun. ACM, 48*(10), 99-104.

Li, F. (2003). Implementing E-Government Strategy in Scotland: Current Situation and Emerging Issues. *Journal of Electronic Commerce in Organizations, 1*(2), 44-65.

Lu, M.-t. (2001). Digital Divide in Developing Countries. *Journal of Global Information Technology Management, 4*(3), 1-4.

CSO Magazine. (2011). 2011 cybersecurity watch survey: How Bad Is the Insider Threat? *CSO Magazine, January, 1*(1), 1-8.

Matangi Tonga. (2013). *Tonga's high-speed internet goes live august 21*. Retrieved July 25, 2017, from http://matangitonga.to/2013/08/14/tonga%E2%80%99s-high-speed-internet-goes-live-august-21

Ma'u, P. (2015). E-Government in Tonga. *Asia-Pacific Regional Forum on e-Government, 1*(1), 1-19.

Miller, C. A. (2004). Human-computer etiquette: Managing expectations with intentional agents. *Communications of the ACM, 47*(4), 31-34.

Miller, B., & Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. *Proceedings of the 1st Annual conference on Research in information technology* (pp.51-56). Canada: ACM.

Meyer, D. (2017). Check Point's 2017 Cyber Security Survey Shows Key Concerns and Opportunities among IT Professionals. *2017 Check Point Software Technologies, 1*(1), 1-3.

Ndou, V. (2004). E-government for developing countries: opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries, 18*.

Nkwe, N. (2012). E-Government: Challenges and Opportunities in Botswana. *International Journal of Humanities and Social Science, 2*(17), 39-48.

Salnitri, M., Paja, E., & Giorgini, P. (2014). Preserving Compliance with Security Requirements in Socio-Technical Systems. In F. Cleary & M. Felici (Eds.), *Cyber Security and Privacy: Third Cyber Security and Privacy EU Forum, CSP Forum 2014, Athens, Greece, May 21-22, 2014, Revised Selected Papers* (pp. 49-61). Cham: Springer.

Seifert, J. W. (2003). A primer on e-government: Sectors, stages, opportunities, and challenges of online governance *Library of Congress Washington DC Congressional Research Service, 1*(1), 1-25.

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., . . . Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications, 34*, 166-182.

Sharma, S. K., & Gupta, J. N. (2003). Building Blocks of an E-Government—A Framework. *Journal of Electronic Commerce in Organizations, 1*(4), 34-48.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., & Flynn, L. (2012). Common Sense Guide to Mitigating Insider Threats. 4th edn. CERT Carnegie Mellon Software Engineering Institute: Carnegie Mellon University.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

United Nations. (2008). *UN E-Government Survey 2008: From E-Government to Connected Governance*. New York: United Nations publication.

United Nations. (2016). *United Nations E-Government Survey 2016: E-government in Support of Sustainable Development.* New York: United Nations publication.

Vespignani, A. (2012). Modelling dynamical processes in complex socio-technical systems. *Nature physics, 8*(1), 32.

Vinod Kumar, T. M. (2017). E-Democracy for Smart Cities: Conclusion and Path Ahead [Vinod Kumar2017]. In T. M. Vinod Kumar (Ed.), *E-Democracy for Smart Cities* (pp. 523-551). Singapore: Springer.

von Solms, S. H. (2010). The 5 Waves of Information Security – From Kristian Beckman to the Present. In K. Rannenberg, V. Varadharajan, & C. Weber (Eds.), *Proceedings of the 25th IFIP TC-11 International Information Security Conference. Security and Privacy – Silver Linings in the Cloud: Held as Part of WCC 2010* (pp. 1-8). Brisbane: Springer.

Walker, E. T. (2015). The politics of information: Problem definition and the course of public policy in America. *Interest Groups & Advocacy, 4*(3), 297-301.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security* (5ed.). USA: Cengage.

Whitworth, B. (2009). A brief introduction to sociotechnical systems. In *Encyclopedia of Information Science and Technology, Second Edition* (pp. 394-400): IGI Global.

Whitworth, B., de Moor, A., & Liu, T. (2006). Towards a Theory of Online Social Rights. In R. Meersman, Z. Tari, & P. Herrero (Eds.), *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops: OTM Confederated International Workshops and Posters, AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET, OnToContent, ORM, PerSys, OTM Academy Doctoral Consortium, RDDS, SWWS, and SeBGIS 2006, Montpellier, France, October 29 - November 3, 2006. Proceedings, Part I* (pp. 247-256). Berlin: Springer.

Willoughby, M., Gómez, H. G., & Lozano, M. Á. F. (2010). Making e-government attractive [journal article]. *Service Business, 4*(1), 49-62

Woodson, T. S. (2016). Public private partnerships and emerging technologies: A look at nanomedicine for diseases of poverty. *Research Policy, 45*(7), 1410-1418.

Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Li, J. (2015). Survey on cyberspace security. *Science China Information Sciences, 58*(11), 1-43.