Data Security Assessment for Organisations in Tonga

Siuta Laulaupea'alu and Te Taka Keegan

Department of Computer Science, University of Waikato, Hamilton 3240, New Zealand
siuta.laulaupeaalu@waikato.ac.nz; tetaka@waikato.ac.nz

Abstract. This paper summarises results from a data security assessment that was undertaken in Tonga in June and July 2016. The assessment investigated Tongan organisations and departments at the Government of Tonga to determine cybersecurity awareness and strategies. Issues analysed included methods of storing and protecting sensitive information, assessing vulnerabilities and threats encountered, and action to counteract cyberattacks on existing computer systems. This paper begins by explaining how the installation of fibre optic cable in Tonga brings advantages and disadvantages to the nation. The methodology describes the approach carried by the researcher to gather cybersecurity data from the survey participants. A SWOT analysis follows to highlight the strengths and weaknesses of this particular research. The survey findings are summarised in broad terms and then further discussed under general findings, positive findings and negative findings. The results of this research highlight some of the major areas that need to be addressed in Tonga. Computer systems are currently vulnerable, and hackers are able to attack these systems from several different angles. This is something that has been noted by the Government of Tonga and steps are being taken to address the inadequacies.

Keywords: Cybercrime, Cloud Computing, Two Factor Authentication.

1 INTRODUCTION

In 2013, the Kingdom of Tonga connected to the Southern Cross submarine fibre optic cable network. The cable connection is routed around Hawaii, Fiji, New Zealand, Australia, and the west coast of the United States of America [12]. The 826-kilometer undersea cable connection from Tonga to Fiji was funded by a grant from the Asian Development Bank, World Bank, and the Tonga Communication Corporation. The preliminary aim of this multi-million-dollar project was to support the people of Tonga by reducing their internet costs. For three decades Tonga experienced high satellite internet costs. The Tongan people were delighted with the new technology and its reduced costs [7].

The other aim of this multi-million-dollar project was to change from a low speed to a super-fast internet connection speed. In August 2013, the internet speed was switched from 20 - 30 megabytes per second to 10 gigabytes per second. Faster internet speed is considered an attractive factor for getting more business and more internet users. The current internet speed is faster than the previous satellite network and "greater than many urban communities in the United States get" [2]. At the same time, Tonga provided incentives for its people to be able to access the new broadband network connection. The Government of Tonga (GoT) offered fifty percent discount on service to hospitals and schools, including the University of South Pacific (Tonga) [2].

As the number of internet users grows at a rapid pace, there is more likely to be a high number of issues to be resolved. The success of the GoT Internet incentives raises a number of important concerns. Cybercrime is one of these major concerns, as attackers will target the new connectivity and availability to exploit internet users in Tonga. According to Matangi Tonga Online, the high-speed internet brings opportunities such as job and business but it "also brings malicious cyber actors who can target victims in the region**"** [4].

2 METHODOLOGY

The research described in this paper was undertaken as part of a Master of Cyber Security Master's Degree at the University of Waikato in 2016. A *Quantitative Research Method* (QRM) was chosen as the appropriate method for this project. The researcher (Siuta Laulaupea'alu) spent 33 days in Tonga to undertake user studies, Monday 13 June 2016 to Friday 29 July 2016. Participants were informed about the importance of telling the truth and answering the questions as accurately as possible. Failure to provide right answers may lead to wrongly identifying the real problem with Tonga's computer security system. Participants were instructed to answer questions that they knew and avoided using assumptions. For questions that they did not know, the answers to "N/A" were used.

The target participants were selected from the main central areas of Information Communication Technology (ICT) development in Nuku'alofa the capital of Tonga. The other participants were randomly chosen from Vava'u, the second largest island in Tonga. A total of 63 participants were involved in this survey. About 31 participants (49 percent) were from Government Ministries, 13 participants (21 percent) from Public Enterprises, 4 participants (6 percent) from banks, 3 participants (5 percent) from agencies/boards, 2 participants (3 percent) from schools, and 10 participants (16 percent) from another organisations/public. All the questionnaires were hand delivered by the researcher to the participants. The researcher first explained the purpose of the survey before handing the questionnaire to the participants. The questionnaire consisted of multiple choice, open-ended, and gap-filling questions based on Network Access, Data Backup & Storage, Organizational Security Management (OSM), Penetration Testing (PT), Disaster Recovery Plan (DRP), Business Continuity Plan (BCP), Two Factor Authentication (TFA), password, Information Security Policy (ISP), data encryption, anti-virus, cyber insurance, and general cybersecurity questions. Most of the participants filled out the questionnaires and returned them independently. Approximately one quarter of the participants needed assistance to understand and complete the questionnaire.

All the questions from the questionnaire were entered into an Excel Spreadsheet for analysis. The data were converted to statistical data and then transformed into tables and charts. Comments was placed underneath the figures/tables for easier reading and understanding. The conclusion and recommendations were based on the analysed data and highlighted significant flaws in cyber security awareness and protection.

3 SWOT ANALYSIS

SWOT, an acronym for Strength, Weakness, Opportunity, and Threat. It is a useful technique for developing a strong strategy plan for resilient businesses or projects. SWOT analysis covers the project greatest strengths, weaknesses, opportunities, and threats [10]. Strength and weakness are internal characteristics within the process (location, patent, and reputation); these need constant monitoring as they can be altered at any time. Opportunities and threats are external to a business or project (competitor, supplier, price); while they still need to be monitored it is less likely they can be altered by the business or project itself. A SWOT analysis is used here to discuss various aspects of the research project that was undertaken on cybersecurity in the Kingdom of Tonga.

3.1 Strengths/Advantages

Surveys are able to be administered in different modes, such as email surveys, online survey, paper surveys, face-to-face interviews, telephone interviews, or questionnaire surveys. The modes selected for this research were a questionnaire and face-to-face interviews with the participants. These modes are flexible and are relatively inexpensive, important factors for the Tongan environment.

The researcher was able to establish a close a connection between the researcher and the participants. This is because the researcher, who was also the interviewer, was Tongan himself. Consequently he was familiar with the people and he understood the cultural and social expectations and responsibilities. The survey was in English but the interviewer was able to introduce himself and

the research to the participant in the participant's native tongue. Queries about the questionnaire or the research were answered in English or Tongan and as such, were easier to understand for the participants.

The sharing of native language helped the participants to understand and provide accurate answers to the questionnaire. Technical terms that were used in the questionnaire were able to be explained in a familiar language to the participants. Participants were invited to write the answers in their own language of Tongan if they had difficulties with the English language.

3.2 Weaknesses/Disadvantages

A major challenges of this project was keeping the collected information confidential and secure. From a participant's perspective, they must be assured information is well secured and kept confidential. Leaking confidential information may lead to a loss of trust with the participants and between the Government of Tonga, the interviewer, and the University of Waikato (UoW). To keep a strong working relationship between all involved, all information was controlled and kept as securely as possible. To solve this issue, all questionnaires were locked in a home cabinet until the analysis tasks were completed. The questionnaires were then passed on to the UoW for secure storage.

As the question was written in English and used technical words, participants must be literate in English and computer literate to have a fair understanding of the terminology. The questionnaire consists of technical words that may seem a mystery to some of the participants. Although some of them can read in English to some degree, comprehension may be restricted by technical terms. Language is also a major barrier, as participants must be able to read and write fluently in English. To solve this issue, the interviewer spent time with the participants to answer queries, in Tongan language, about the questionnaire. For those who needed more time to go through the questionnaire, the interviewer was happy to return and help.

The participants wanted to look competent and knowledgeable and sometimes pretended to know all the answers. Failing to complete all questions may have seemed to suggest they were not capable enough and may have seemed to result in a lowering of their moral status. This perception leads the participants to feel they must complete the questionnaires due to the pressure of looking good, and put on their own idea spin to the response so that it makes them look better [5]. Because a face to face interview strategy was used the interviewer was able to notice and manage this issue and to foster a more accurate response from the participant.

3.3 Opportunities

Cyber security appears to be a new topic in Tonga and in the Pacific Nations. Cyber-risk is leading at the top of the world agenda due to high profile breaches and increased fears that security failures and hack-attacks must be engaged in the global economy. "In Australia, cybercrime costs businesses more than $600 million a year, while in the US, one in five online consumers have been victims of cybercrime in the last two years, equating to $8 billion" [9]. There are great opportunities to introduce and understand cybersecurity and cybercrimes on a worldwide basis. The likelihood of cybercrimes to spread in Tonga and Pacific nations must be a target for the attackers due to limitations of resources and preparedness deficiency. A lack of concern by Governments or set strategic plans, give rise to concerns around the opportunities that exist for cybersecurity threats. Hence this research was an opportunity to increase awareness by the government and people of Tonga to cybersecurity threats.

The cybersecurity threats also offer opportunities for research and study in areas to combat the threats. Many universities and tertiary institutions are offering courses and degrees in cybersecurity, such as the University of Waikato's (UoW) Cyber Security Lab. Students of the Pacific Islands that complete trainings and course in these degrees will be in a position where they can return to their home islands and assist to combat these threats. An unexpected benefit of this research was to make people of Tonga aware of the study opportunities in cybersecurity.

3.4 Threats

There were two initial threats to this research project being undertaken. Would the Government of Tonga support the intentions of the research and allow the research to be undertaken in its departments? Would the participants be willing to respond to the questionnaire and have their responses and interviews completed in the time frame that was allocated to the interviewer. The initial threat was quickly allayed as the GoT quickly came on board and was very supportive of the research. Most of the participants reacted fast and honoured their words of handing in the questionnaires on time. However some, while responding in a friendly manner, were delayed in completing questionnaires, and some did not make in the allocated time frame. This may have been because the language of the questionnaires was new to them. Ultimately though, good numbers of questionnaires and participants were reached.

4 SURVEY FINDINGS

This section consists of two parts. The first part is represented by charts that were taken from survey findings in order to make a clearer picture of the survey results. The second part highlights some of the areas that required attention from the kingdom of Tonga. The survey was conducted with 63 organisations in Tonga. All the survey findings are taken from the author's unpublished thesis submitted to the University of Waikato in 2016 [11]

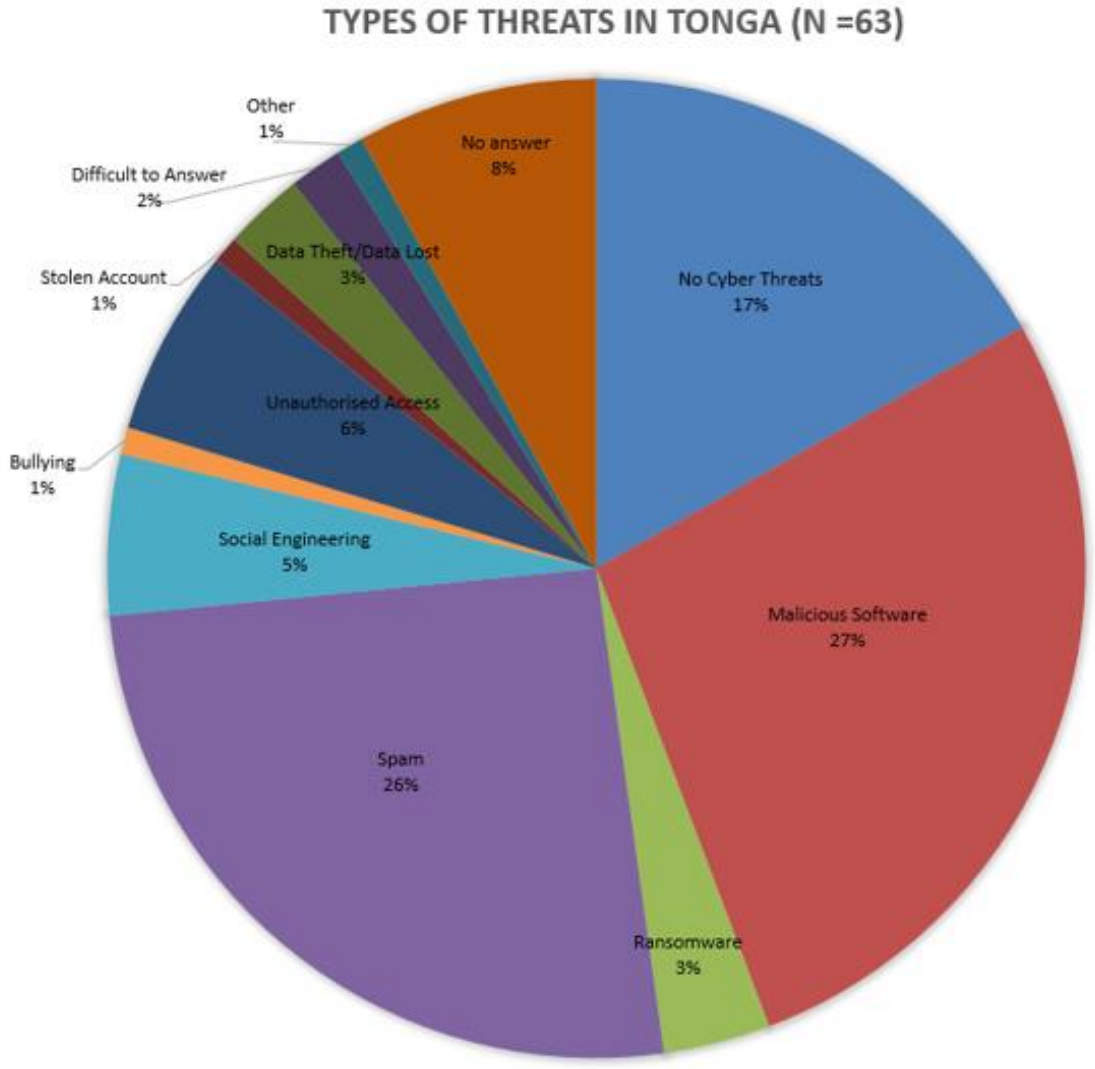

Fig 1: Cyber-threats in Tonga.

The survey findings discovered that Tongan organizations were vulnerable and victims of cyber-threats/cybercrimes. About 73 percent of the organizations in Tonga had been exposed to cyber-threats and cyberattacks as summarised.

Figure 1 reveals that at least 27 percent of the organizations have been victims of malicious software, 26 percent have been victims of Spam, 6 percent have been victims of Unauthorised Access, and 5 percent have been victims of Social Engineering. It also shows 3 percent have been victims of ransomware, 3 percent have been victims of data theft/data loss, 1 percent is bullying, 1 percent is stolen account and 1 percent is for another type of crimes. It is only 17 percent of the organizations have not been victims of cyber threats and cybercrimes, 8 percent did not answer the question and 2 percent had difficulty in answering the question. In summary, at least 73 percent of Tonga's organizations are victims of cybercrimes and cyber threats.

The study also revealed that 51 percent of the Government computers were not encrypted, 53 percent of users were not aware of Penetration Testing (PT) or Pen Testing and 64 percent were not using cyber insurance. In addition, a significant portion (44 percent) of the organizations were not aware of Two Factor Authentication (TFA).

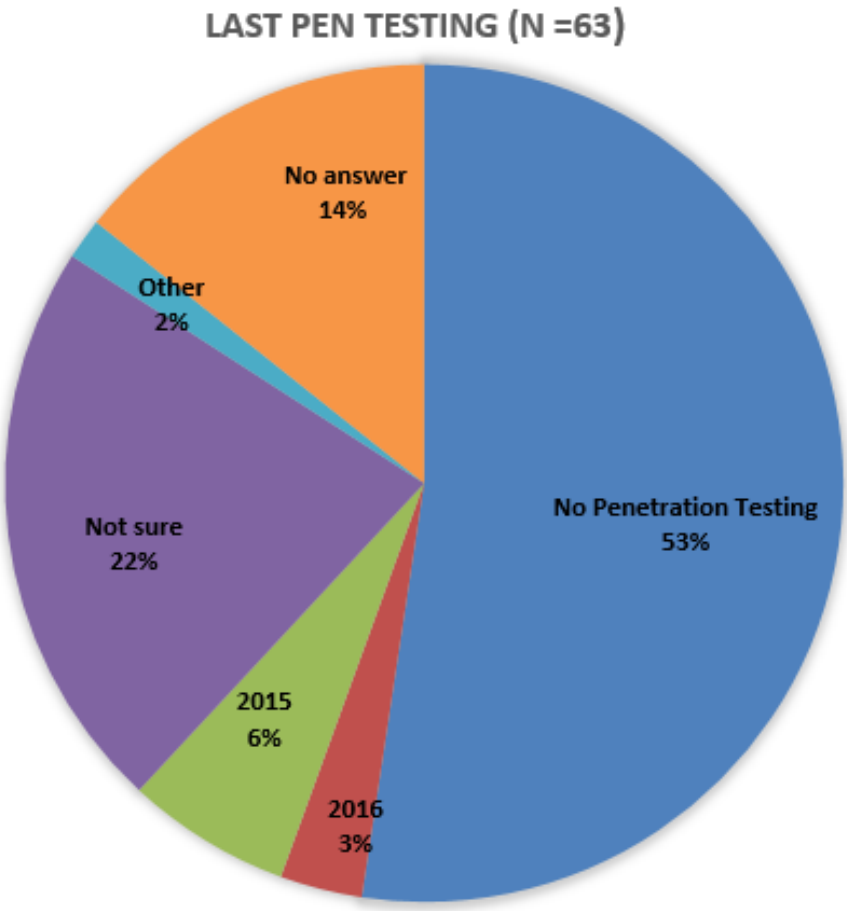

Fig 2: Last Penetration Testing

Figure 2 shows that the majority (53 percent) stated that no Penetration Testing ever took before and 9 percent of the organizations carried out PT in 2015 and 2016. It also shows that 22 percent were not sure, whether they carried out PT or not, 14 percent did not answer the question and 2 percent provides "Other" answer for the question due to organizations restriction to release any information. Furthermore, only 8 percent was deploying Cloud Computing for data storage and backup.

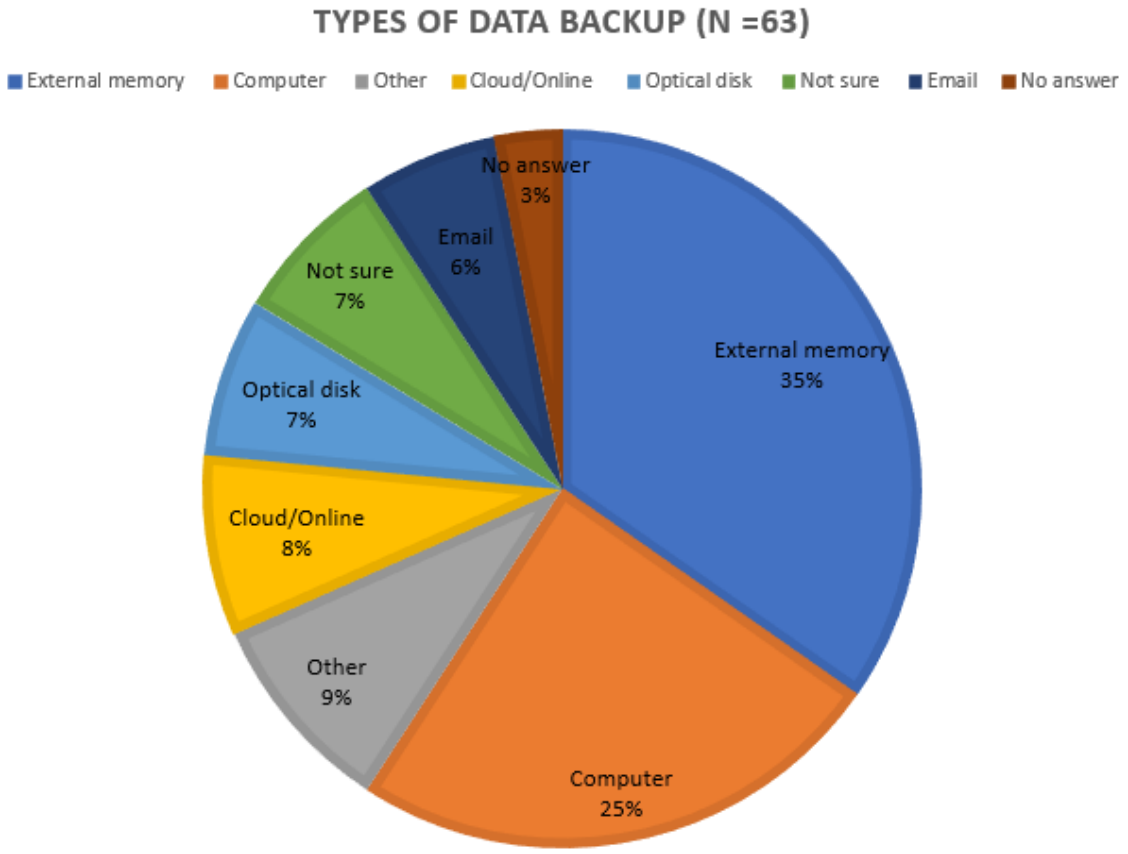

Fig 3: Data Backup Devices

Figure 3 represents the devices used by the organisations for data backup. The External Memory Card or External Storage (35 percent) and Computer (25 percent) are the most popular devices used in Tonga. Only 8 percent of the organizations in Tonga are using Cloud/Online facilities.

The key findings from the survey are divided into three parts: general findings, negative findings, and positive findings. This section highlights some of the key points discovered in the survey.

4.1 General Findings

- The majority of survey participants were from Nuku'alofa, comprising 70 percent, and the remainder of survey participants were from Vava'u, comprising 30 percent. About 75 of the survey participants (75 percent) were from Government ministries, agencies/bodies, and public enterprises and the remaining 25 percent belonged to schools, banks, and other agencies.
- A question was asked to test the participants' understanding of cyber security and cybercrime. It was found that 71 percent were able to answer and explain the meaning of cyber Security and 62 percent were able to answer and explain the meaning of cybercrime.
- A great proportion (35 percent) of the organizations tended to seek help from any person who knows how to combat cyber threat/cybercrime, and 23 percent said that their organization's employees were able to solve cyber security issues internally.
- In terms of data loss, 73 percent of the organizations in Tonga were able to retrieve file/data successfully in terms of unintentional break down of computer system, 14 percent were unable to retrieve file/data and 13 percent did not answer the question.
- Passwords; for the majority (65 percent) of the organizations had not used any words appearing in a dictionary. 60 percent of the users had not inserted personal information such as birth dates or social ID in their passwords.

- The majority (64 percent) of the organizations had enforced a Security Policy (SP) for all employees, contractors, staff, and other people accessing their network, while 33 percent had not deployed an SP, and 3 percent was unable to answer the question.
- Regular scanning keeps the computer systems safe. The highest level (48 percent) of the organizations scan their computer systems daily and 30 percent are scanned weekly.
- Most of the organizations (90 percent) believed that this research is helpful for the future security of Tonga's computer systems. In addition, the majority (67 percent) of the organizations requested a copy of the survey results from this research, so that they could improve their cyber security.

4.2 Negative Findings

- Computer systems in Tonga were vulnerable. The findings revealed that 73 percent of the organizations in Tonga had been victims of cybercrimes and cyber-threats (Malicious Software, Social Engineering, Ransomware, Data Theft/Data Lost, Spam, Unauthorized Access, and Others). The top four cyber threats discovered in Tonga are Malicious Software (27 percent), Spam (26 percent), Unauthorized Access (6 percent), and Social Engineering (5 percent).
- Online storage and online backup are recommended by security experts as one of the most secure techniques available. The survey revealed that only 8 percent of the organizations in Tonga started to deploy Online/Cloud storage to back up their sensitive information and important data.
- Data encryption was one of the most effective techniques to secure data. The survey revealed the majority (51 percent) were storing sensitive information/files on servers and databases that were not encrypted. Without data encryption, the files/sensitive information could be altered/intercepted by outsiders.
- The greatest proportion (44 percent) of the organizations were not using another layer of security, such as Two Factor Authentication (TFA), to access their systems. Only about 21 percent were using TFA and 19 percent of the organizations do not understand TFA.
- It was found that 43 percent of the organizations in Tonga indicated that they had not upgraded their anti-virus software for 12, 18, 24, or more than 24 months; had never upgrade the anti-virus; or had no answer for this question. Although it was not the majority of the organizations, it is a concern that so many organizations did not upgrade their antivirus software.
- One of the new areas discovered in the survey was Penetration Testing (PT). The majority (53 percent) of the organizations in Tonga were not carrying any PT for their systems. Also, 64 percent of the organizations were "Not sure" when they are going to carry out their next PT. Furthermore, 41 percent of the organizations were "Not sure" how to plan or conduct PT in the future.
- The idea of cyber insurance was also new. According to the survey findings, the majority (64 percent) of the organizations in Tonga did not deploy cyber insurance. Only about 5 percent deployed cyber insurance and 46 percent did not provide any answer to this question.
- A question was asked the participants: "Were any loopholes or security threats found in your organization last Penetration Testing (PT)? The greatest proportion (46 percent) provided no answer and 33 percent also preferred not to answer the question. It also showed that 18 percent found no loopholes found in their system, but only 3 percent did find loopholes in their last PT.
- The majority of the organisations (63 percent) said "No" that no disaster ever damaged their data/files/records and 24 percent informed they got an attack with disasters/attacks. The remaining 13 percent did not provide an answer to this question as Disaster Recovery Plan (DRP) or Business Continuity Plan was new in Tonga.
- The majority (51 percent) explained that their organizations were not satisfied ("No") with the response from Insurance Company about their insurance claims. It was only 9 percent of the organizations who were satisfied with the respondent about their insurance claims. The remaining 40 percent of the organizations was not able to answer the question

4.1 Positive Findings

- Most of the organizations (89 percent) had installed a firewall to protect their systems from viruses, worms, hackers and other types of attacks, and the majority (92 percent) had also installed antivirus protection.
- The top five antivirus systems used were AVG (22 percent), McAfee (16 percent), Norton (14 percent), Malwarebytes (11 percent), and Avira (9 percent). The organizations normally scanned their systems every day (the greatest proportion at 48 percent).
- The organizations set up clear job descriptions to outline the security responsibilities for all personnel. The majority (62 percent) of the organizations used clear job descriptions to define security responsibilities for all staff and employees.
- To access the internet, employees, staff, contractors, and people must adhere to the Security Policy (SP) provided by the organizations. The majority (64 percent) of the organizations agreed that SP must be enforced. Also, most of the organizations (89 percent) agreed that accessing the internet led to security vulnerabilities.
- The authentication process is set to verify the correct username/password to log into the computer system. Users have to log in with the correct credentials within a certain number of attempts. The survey revealed that the highest level (41 percent) of the organizations set 1 – 3 attempts to log into their accounts. If the users failed to input the correct password within 1 – 3 attempts, then the accounts would be blocked.
- The survey showed that most (38 percent) passwords contain a mix of digits and characters, and 35 percent contain a mix of digits, characters, and others (e.g. symbols and punctuation).
- About 89 percent of the organizations in Tonga were aware that accessing the internet leads to security vulnerabilities that may harm their computer systems.
- The majority (33 percent) of the organisations in Tonga were using Microsoft Access as the most popular database. Other database such as MySQL (20 percent), Microsoft SQL Server (20 percent), Oracle (4 percent), and Apache Derby (1 percent) were also used. The other organisations (11 percent) used other types while others (11 percent) were unable to know the types of database used.
- The majority of the organisations (67 percent) were aware of the security risks related to the database. Only 24 percent are not aware of security risks/threats, and 9 percent did not answer the question.
- The majority (51 percent) of the organisations deployed Information Security Policy (ISP) to safeguard all parties (Employees & Staff, Managers, Contractors, Third-Party, Visitors, Others) when they access to the workplace.
- The survey revealed that the majority (73 percent) of the organizations agreed that specific people were accountable for their actions/inactions. A small number (6 percent) disagreed that specific people were not accountable. The remaining 18 percentage replied to “Not Applicable” and 3 percent did not answer the question.
- The greatest proportion (27 percent) of the organizations in Tonga were using Cable - Broadband Internet Connection to connect to the internet. It also revealed that 22 percent were using Wireless Internet Connection, 16 percent of the organizations used ADSL - Asymmetric Digital Subscriber Line, and 9 percent used Wi-Fi. The remaining percent referred to other types of connections such as ISDN - Integrated Services Digital Network, B-ISDN - Broadband ISDN, DSL – Digital Subscriber Line, Cellular network (e.g. 3G, 4G), and other types of connections. NB: The leading connection device (Cable - Broadband Internet Connection) relates to the undersea Southern Cross fibre optic cable, connected from Fiji to Tonga in 2013.

5 CONCLUSION

The results of this research highlight some of the major areas that need to be addressed in Tonga. Computer systems are currently vulnerable, and hackers are able to attack these systems from several different angles. Sphere Phishing, Rotary Scams, and ATM Scams existed in Tonga before this research commenced. For example, an ATM Scam was discovered in March 2016, when BSP bank customers had unauthorized transactions on their bank accounts [8]. Another major problem discovered during this research was related to the deposit of money to a false Bank account. Such cybercrimes/cyberattacks are predicted to increase in the future unless the appropriate security controls are implemented. Awareness of and familiarity with Penetration Testing, cyber insurance, Disaster Recovery Planning, Cloud Computing, and Business Continuity Plan were limited. These areas need to be better understood within Tongan organizations.

Tonga has now begun to take steps to improve cybersecurity. The Computer Emergency Response Team (CERT) was launched in Tonga in July 2016, making it the very first island in the Pacific to establish a National CERT. Their preliminary work with ICT related incidents, such as applications and hardware failures, hackings, computer viruses, data leakages and other security vulnerabilities. CERT has therefore played a significant role in keeping the whole system safe, as the number of internet users has exploded [6]. The GoT had passed the "Communications Commission Act and Communication Act 2015" [3] to enforce cyber security and to protect Tonga from the negative effects of the internet.

The survey identified security threats and weaknesses in Tonga's computer systems. It should be treated as a "wake-up call" for the Government and the people of Tonga to address security issues. In response to this survey, the GoT reacted quickly to some verbal discussions between the researcher, the GoT, and the University of Waikato. To formalise a strong working relationship between these two parties, the former Deputy Prime Minister of Tonga, Siaosi Sovaleni, came to the University of Waikato and signed a Memorandum of Understanding in May 2017 [13].

> *"Both parties agreed to work on capability building, research collaborations, and staff and student exchange – aiming to ensure the success of the lab's STRATUS project, the Tongan government's E-Government project and the Tonga National CERT. This work builds on Siuta Laulaupea'alu's thesis work who recently graduated with a Master in Computer Science from the university. Through Siuta's project, we were able to develop great synergies and a strong collaborative spirit. This MoU will enhance the ability of both organisations to leverage on Waikato's cyber security research breakthroughs in data provenance, cyber security visualization, situation awareness, and applications of homomorphic encryption"* [13].

The research was undertaken to raise awareness about the increasing number of cybercrimes happening globally and subsequently its influence on the people of South Pacific including Tonga. This research is very important to identify the cybersecurity position of Tonga and the result of this survey indicates that Tonga are vulnerable. The GoT needs to work on these issues to protect the people from the exploitation of cyber-attackers and cybercriminals.

The responsibilities of the GoT, the researcher, and the people of Tonga are to ensure that Tongans are in a safe environment, and that our children will not blame us due to our negligence and non-preparation for the future. We are not able to stop computer disasters and cybercriminals, but there are several techniques that can protect users, as "Prevention will always be your best line of defence against cyber criminals" [1]. Prevention is better than cure.

6 REFERENCES

[1] Eskola, M. (2012). From risk society to network society: Preventing cybercrimes in the 21st century. *Journal of Applied Security Research*, 7(1), 122-150.

[2] Mark Hay. (2014) *Here's how a tiny Pacific Island got better Internet than the US.* from https://www.pri.org/stories/2014-08-01/heres-how-tiny-pacific-island-got-better-internet-us

[3] Matangi Tonga Online. (2016). *CERT team aims to protect Tonga from cybercrime*. from https://matangitonga.to/2016/07/22/cert-team-aims-protect-tonga-cybercrime.

[4] Matangi Tonga Online. (2017). *Workshop held in Tonga to combat cybercrime*. from https://matangitonga.to/2017/05/24/workshop-held-tonga-combat-cybercrime.

[5] Mind Tools. (2016). *Thinking on your feet*. from: https://www.mindtools.com/pages/article/ThinkingonYourFeet.htm.

[6] Ministry of Information and Communication.(2016). *PM launched Tonga National CERT*. from http://www.mic.gov.to/news-today/press-releases/6159-pm-launched-tonga-national-cert.

[7] Pacific Media Centre. (2013). New high speed internet cable arrives to go live in August. from: http://www.pmc.aut.ac.nz/pacific-media-watch/tonga-new-high-speed-internet-cable-arrives-will-go-live-august-8327.

[8] Rita Narayan. (2016). *Tonga bank customers hit by Fiji ATM targetted scam.* from http://www.looptonga.com/content/tongan-bank-customers-hit-fiji-atm-targetted-scam.

[9] Saini, H., Rao, Y. S., & Panda, T. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, 2(2), 202-9.

[10] Sevkli, M., Oztekin, A., Uysal, O., Torlak, G., Turkyilmaz, A., & Delen, D. (2012). Development of a fuzzy ANP based AWOT analysis for the airline industry in Turkey. Expert systems with Applications, 39(1), 14-24

[11] Siuta Laulaupea'alu. (2016). *Data Security Assessment for Government Information Systems in Tonga*. Unpublished Master Thesis, University of Waikato, Hamilton.

[12] Southern Cross Cable Network. (2012) *Overview and Map* 2012. from: https://www.southerncrosscables.com/home/network/overviewandmap.

[13] The University of Waikato. (2017). *Government of Tonga and Waikato cyber security collaboration*. from: http://www.waikato.ac.nz/news-events/media/2017/government-of-tonga-and-waikato-cyber-security-collaboration.