Cyber Security Vulnerabilities in Tonga

Siuta Laulaupea'alu[1] and Te Taka Keegan[2]

Department of Computer Science, University of Waikato, Hamilton 3240, New Zealand
[1] sl258@students.waikato.ac.nz; [2] tetaka@waikato.ac.nz

Abstract. A research project undertaken in Tonga in 2016 showed that Tonga's computer systems are susceptible and can be easily exploited by cybercriminals. This paper builds on that research by identifying areas of vulnerability and then recommending how these vulnerabilities can be addressed. Areas discussed include penetration testing, a data recovery plan, budget considerations, cyber insurance, the employment of cyber security experts, information security policies, data encryption, the backing up of data, two factor authentication, the integrity of passwords, and database considerations. By detailing and discussing these issues it is hoped that an awareness can be raised by organisations and government departments of Tonga and that the people of Tonga can best prepare themselves for the increase in cybercrime and cyberattacks that is likely to occur in the Pacific.

Keywords: Cyber Threats, Cyber Insurance, Cloud Service Provider.

1 INTRODUCTION

In 2016 research was undertaken by the author[1] around cyber security issues in Tonga. A major breach that was discovered related to misinterpretation and lack of knowledge about a bogus email. An email was sent from an illegitimate source asking one of the large government organisations to pay a bogus bill. The email appeared to be real and trustworthy. The government organisation agreed to deposit a large amount of money into a bank account. Investigations were carried out, but the government organisation never identified where this fake email came from [28].

A Tongan phrase says: "Kapau kuo vela e 'akau mataa pea huanoa e 'akau momoa". The English translation for this phrase is as follows: If the green trees (living trees) are fast/easy to burn then how about the firewood (dead trees)? In regard to this case, it refers to the well-educated people and government representatives who use the Internet a lot. They have more Information Technology (IT) experience than other non-civil servants and supposedly belong to the 'green tree' level. But they were still caught in this trap, they were 'fast/easy to burn'. The authors have concerns for the computer illiterate people, the 'firewood' level, and the common people that are beginning to use on-line resources who have a lack of awareness about cybercrimes. The authors suggest that the Government of Tonga (GoT) focus on vulnerabilities that affect the 'firewood' as these people are the most likely to be burnt the quickest and the most by cyber-attackers.

2 CYBERCRIMES IN TONGA

The bogus email that happened in Tonga identified some of the real implications of the lack of IT knowledge of Tongan government representatives. These people are in the 'green tree' level and trusted within the community due to their education and job status. They deal with emails and gain experience with IT related works in their workplace every day but were still caught out by a relatively simple online scam. The 'firewood' level (dead tree or 'akau-momoa) are obviously more susceptible due to their lack of IT understanding, which is likely to allow more opportunities for scammers. The fake email scam and the significant amount of money lost in this scam highlights that Tonga is vulnerable to cyber-attacks.

Further cybersecurity issues have been revealed in Tonga. The NZ Kaniva website reported on March 2016, that some Tongan customers of BSP bank have reissued new cards after their cards were

blocked [13] [24] [28]. This problem is known as an ATM scam, and it is believed that the problem initially started in Fiji and then spread over to Tonga. An announcement from the Tonga National Reserves Bank (TNRB) [24] confirmed that the ATM scam was caused by criminal activities. Customers were affected by unauthorized transactions on their bank accounts. TNRB has informed local customers that if they have withdrawn or deposited money in Fiji within the last 12 months, they are likely to be victims of this ATM scam. The concern is for the customers who had used VISA cards at ATM machines [24] [28]. An electronic device, also known as a skimming device, is secretly plugged into an ATM machine. This device gets a pinhole camera to record the customer's PIN number when the customers swipe or insert their cards into the ATM machine [27]. Another technique used by skimmers is by standing with a camera from a far-away location to record finger movement on the ATM machine when customers enter their pin number.

The TNRB informed Tongan cardholders who had been to Fiji to reconcile their bank statements and check bank account balances to ensure their accounts remain unchanged. The result of this scam affected the customers of Bank South Pacific (BSP) and other local bank customers in Tonga. For customers that were affected by this problem, BSP was ready to reimburse the unauthorized withdrawals to customer's bank accounts and reissue new bank cards [13] [24] [28].

Again, Tonga Ministry of Information & Communications also confirmed that Sphere phishing is well known in Tonga, as people receive emails from friends or people they know [21] [28]. The hackers target people who are traveling, by trying to obtain email passwords when the travelers log on to the Internet through a computer system in their hotel. The hackers then infect that person's email account with malicious software that detects all movements on keyboards, including passwords entered by the traveler. As the hackers get access to email accounts, they send emails to all recipients on the victim's contact lists, to tell them their wallets have been stolen and they need funds as they have no other source of money. They play on people's emotional feelings and ask them to help by sending money. The best solution is to contact related families to check if travelers are really in trouble or to call and speak directly with them [21] [28].

3 VULNERABILITY IN TONGA

Tonga is vulnerable to cybercrimes and cyberattacks in according to the author's[1] survey findings discovered in 2016.

> *"The survey results reveal that at least 27 percent of the organisations 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 organisations 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 organisations are victims of cybercrimes and cyber threats"* [28].

As Tonga's computer systems are susceptible and can be easily attacked, the authors recommend the Government of Tonga (GoT) start implementing measures to address the security weaknesses in their systems. Failure to act quickly on these vulnerabilities will lead to a higher number and greater depth of cybersecurity attacks. Suggested recommendations are detailed in the next section of this paper.

4 RECOMMENDATIONS

This section provides recommendations for organisations in Tonga, including the GoT, to implement security measures to maintain a secure workplace and protect their computer systems from cybercrimes and cyberattacks. The security guidelines are based on research undertaken in Tonga in 2016 [26] and in particular from a section titled, 'Negative Findings', which outlined the weaknesses discovered in this survey. Selected "Positive Findings" are also considered, as some of these issues are very sensitive, and must be monitored closely/regularly. The views and recommendations of the author[1] are also informed by face-to-face discussion with the participants, which enabled the researcher to learn real life problems organisations experience within the Kingdom of Tonga. Some of the security vulnerabilities found in the survey are outlined below, and the recommendations for security controls to be set up are indicated.

4.1 Penetration Testing (PT)

Penetration Testing (PT) is a fundamental area of information system security engineering [20], and is a recommended initial process to be undertaken. As the majority (53 percent) of the organisations are not yet utilizing this important task, this action requires immediate implementation. Regular testing demonstrates the weakness in the application and infrastructure. Any loopholes in the IT infrastructure can be located and security measures put in place to ensure no attackers exploit the computer systems. Penetration Testing, also known as Pen Testing, Security Testing, or Network Penetration Testing, is a practice of looking for vulnerabilities in the application (software), infrastructure (hardware), and people. Its purpose is to find vulnerabilities and loopholes that attackers may use to be able to gain unauthorized access to computer systems. A Pen Tester (person taking PT) must first get permission from the Government of Tonga to carry out this task. The Pen Tester attacks in the same way as the attacker, but there is no harm to the computer systems.

Penetration Testers are also known as "white hat" hackers or "ethical hackers" [33] and undertaken "black box testing" [35]. This practice offers the advantage of telling the system owner about security vulnerabilities to fix before the "black hat" hackers exploit the system. The lack of PT experts in Tonga is a major issue. Hiring experts is going expensive. However, the amount of money paid to an expert to carry out PT is significantly less and preferable to any loss or damage that may be caused by the black hat hackers. According to Career-New Zealand website [3], PTs are usually earning NZ$92,000 to NZ$137,000 annually. The GoT is to decide to hire an expert from New Zealand (or other overseas countries) to test loopholes and potential security vulnerabilities. An experience PT can spend few days in Tonga to carry out this task at a reasonable price. It is recommended that PT is carried out on a regular basis to avoid potential damages and significant loss in the future.

4.2 Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)

The Disaster Recovery Plan (DRP) can also be referred to as the Business Process Contingency Plan (BPCP) or Business Continuity Plan (BCP). The DRP is a pre-emptive document designed to support an organisation to maintain ICT information and restoring data assets before, during, and after disaster [7]. The deployment of a DRP was only 35 percent. Also, a total of 33 percent of the organisations in Tonga were "Not Sure" of DRP or BCP and 13 percent did not answer the question. The main reason for the high level of "Not Sure" and "No Answer" in the question was because DRP or BCP was a completely new concept for many organisations and departments in Tonga.

DRP or BCP is an increasingly important feature of computing systems. It consists of protections to maintain the level of security, and a quick resume of operations whenever there are intentional or unintentional cyber security strikes or other kinds of damage to IT infrastructures. DRP not only focuses on disaster prevention but also includes analysis of the continuity needs of IT business processes [19].

4.3 Budget

Some large organisations are not allocating funds in their budget to purchase antivirus software for protection against malicious software like viruses, Trojans, and worms. The survey revealed one of the reasons that organisations are unable to upgrade their antivirus software is due to insufficient or nil funds being reserves for this expense. Survey participants mentioned that they bring their own devices (such as a personal laptop) to their worksites and they paid for their own protection software. This creates an additional vulnerability as personal antivirus protection may be inadequate.

Antivirus software is very important for the overall security to protect Tongan computer systems. The Government will have to provide a budget to purchase the latest versions of antivirus software and to distribute to all the ministries and organisations. Deployment of the latest version of antivirus software will be able to protect sensitive information, data, hardware damages, and lock-down the computer system functionalities. The authors try to emphasise the point that the financial cost of damages that may occur if the systems are compromised by the attackers will be much higher than the cost of purchasing the updated software. A lot of money will be saved when the updated antivirus software is deployed in comparison to the loss/damages that would occur in future.

4.4 Cyber Insurance

Cyber insurance has been stated as "a promising solution to help firms optimize security spending" [34]. It was clear from the 2016 data collection and survey findings that this was an unknown or new area to organisations in Tonga. Many of the participants asked the researcher what this actually was. The majority of the organisations surveyed (64 percent) said that cyber insurance did not apply, they did not answer the question, or that had not yet engaged in this type of insurance cover. Most organisations agree that data is one of their most important assets. Some organisations believe that data or information is worth more than the equipment that is used to store data [9]. Businesses and organisations agree to transfer part of their cyber-risks to Cyber insurance companies [15] to cover network damages; business interruption; data breaches; restoration of data and hardware; fraudulent fund transfers; notification expenses and regulatory fines; credit monitoring; and damage to an individual or company. When faced with these kinds of threats, cyber insurance is in place to cover and replace any loss that may be occurring. Cyber insurance is therefore recommended to be deployed by organisations and government authorities in Tonga.

4.5 Cyber Security Experts

According to Rowe [25],"Cyber-security education and training as a pervasive element in computing and other related programs is recognized as being an excellent method". Tonga is in need of specialized cyber security experts. The results of the survey showed that only small percent (25 %) of the organisations in Tonga hire a specialist as a member of staff to mitigate threats to organisation's data. A total of 19% of the organisations hired professionals from other organisations, while 5 % hired an overseas specialists. The remaining 51 % took no action, did not know of the action to be taken, or gave no answer to the question as they presumably were unaware how to mitigate data threats in their organisations.

The numbers shown above confirm that organisations in Tonga requires cyber security experts to look after the IT systems of Tonga. The primary roles of the cyber security experts are to protect the organisations from hackers. The costs associated with overseas training are small in comparison to the potential future cost of damage to the business or organisation. Proper training and education will empower high-quality understanding and bring advanced knowledge [8] of security responsibilities. The employees should be given the opportunity to participate and enrol in appropriate security training. Different specializations of training, such as computer infrastructure, cyber security law, Cloud computing, management, and policy are offered that would lead to careers as an IT Security Consultant, Information Security Officer, Security Assessment Consultant, and Penetration Tester [31].

4.6 Information Security Policy (ISP) & ISO

Although the majority (51 percent) of the Tongan organisations deployed an Information Security Policy (ISP), there was a concern for the remaining 49 percent. About 43 percent of the organisations were not able to organise ISP and 6 percent were not be able to answer the question. These proportions are high and need attention. The ISP provides policies to ensure that IT users comply with guidelines and rules to safeguard information stored within organisations, to regulate employees security performances, and to prevent misuse of information security systems [14]. The ISP plays significant roles in outlining the responsibilities and roles of users in regard to ICT security. Without ISP, the possibility that the ICT system would be compromised is significant. Moreover, ISP is required to be operational and functional and to be reviewed regularly in accordance with time, and changes, and upgrades to the ICT system. Each nation has created a set of standards for their own use, according to the type of organisation and workplace. Telarc SAI, a joint system shared by New Zealand and Australia, has created their own ISO to provide expert assessment, system assurance, training, control, auditing, and to improve the efficiency and effectiveness of their performance [29].

The International Standards Organisations has two ISP standards. Both standards (International Standard ISO/IEC 27002 and ISO/IEC 27001) are primarily targeted at keeping an organisation's information safe and secure. These standards help the organisations secure intellectual property, financial information, employees' details, and other information entrusted by other third parties [10]. The differences between these two ISOs are that the ISO 27002 is much more precise and much more detailed. The ISO 27002 is not a Management System (MS), but ISO 27001 is MS. MS refers to the standards used to certify and audit the "Information Security Management System" (ISMS), whereas ISO 27002 is used to access the "Information Security Program" (ISP) [10]. The iso.org website recommends using ISO/IEC 27001 to provide the correct needs for ISMS. An ISMS is a kind of approach (systematic) that assists in managing

sensitive information about an organisation or company (of any large, medium, or small size) to remain secure. It includes the process of risk management, processes, IT systems and people [10]. Both ISP and ISO should be enforced in the responsibilities and duties that are undertaken by an organisation such as CERT of Tonga.

4.7 Data Encryption

According to Tian [32], "data encryption in the Cloud environment is a good way to mitigate security concerns over evidence data integrity, preservation and confidentiality by the Cloud". Encryption is an effective method of data protection (security). Encryption is an appropriate method for securing sensitive information to send data to the network, the internet, Cloud, or any sort of device ('data-in-transit'), and to store data or save it ('data-at-rest') in any form or device. Amazon Virtual Private Cloud (VPC) "protects data-in-transit, but does nothing for data-at-rest" [26]. Data is encrypted and decrypted using an encryption key to view the data (file/message) in its original form. Without providing the right key, encrypted data is unable to be decrypted. Unauthorized users and attackers, therefore, are unable to retrieve the original data.

It is important that this sort of protection is implemented in Tonga, as the majority 51% of the organisations are not encrypting sensitive information stored in files, database, and servers. According to Moia [22], cryptography is an effective anti-forensic tool for the protection of information from unauthorised access. Encryption assists forensics experts to recover valuable information and helps in "investigation due to some traces left in the operating system, known vulnerabilities in the tools used, weak choice of passwords by users etc." [22]. It is therefore recommended that data encryption is implemented to protect sensitive information.

4.8 Data Backup

The majority of Tongan organisation's backup data is an external media e.g. SD cards, USB drives, external hard disks, and memory sticks. Online/Cloud storage is more effective, but only 8% of the organisations use this type of backup. According to Abdollahzadegan [1], "Cloud computing is now growing rapidly and organisations of all shapes and sizes are adapting to this new technology". Moving to Cloud storage is an option to hand over the GoT data to be controlled by Cloud Service Providers [CSPs]. CSPs such as Google, Microsoft, Amazon, Sun Microsystems, and IBM have established various data-centres to deploy Cloud computing services in several places around the world to "provide redundancy and ensure reliability in case of site failures" [2].

However, not all commentators agree that CSPs are the best solution for data backup. Kulkarani [16] suggests that the issue of handing over important data to CSPs or other companies is "worrisome" [16]. Tian suggests CSPs are commercial enterprises which "cannot be fully trusted" [32]. The GoT is to decide whether Cloud computing is an appropriate option to be engaged with but the authors recommended to implement Cloud computing as soon as possible. The advantages of cloud computing are utilised internationally and a lot of organisations enjoy Cloud services. For instance, Cloud computing services offer a reduction in IT-related costs on implementation, maintenance, hardware, power, cooling, and operational [4] to make more attractive, convenient and affordable for internet users.

4.9 Two Factor Authentication (TFA)

Multi-layered protection provides different levels of safety against imported material [5]. According to Jin [12], "the most practical way of addressing the privacy invasion problem is to combine two or more factor authenticators". Associate Professor Ryan Ko, the director for New Zealand Institute for Security and Crime Science, and Head of Cyber Security Lab at the University of Waikato, New Zealand, also stresses the importance of multi-factor authentication: "the more authentication stages on your account, the harder it is to hack" [30]. Another new finding discovered in Tonga is that only 21% of organisations use an extra security layer, TFA, to access files/systems. Using strong password settings as described above does not guarantee full safety as the password may be compromised at any stage. TFA adds on another login (apart from the user's normal login) to access files/accounts. The first normal login to the system uses usual credentials, and then another field/page prompts the user to log in using either a security question or a One Time Password (OTP). The OTP is received through email or a mobile phone, this code or number must be entered into the second login page. It is also important to add another backup mobile number for a standby verification code if the original mobile number is not available. TFA is optional, but from a security perspective, it is highly recommended that it be used.

Data Encryption (section 4.7) and Two Factor Authentication (TFA) discuss the process of setting security mechanisms to secure data in the Cloud. Data Encryption and TFA can be considered as part of Cloud computing security processes but depend on the users' choice. CSPs are committed to providing the best services, IT security resources, industry certifications, and the security standards. Therefore the users are one hundred percent assured their data are well secured. Cloud storage is believed to be a convenient method of data storage and data backup. Encrypted files are sent to the Cloud and TFA is then used to access them.

4.10 Password Renewal & Password Setting

The number of days for password renewals is between 30 days to 80 days. About 47 percent of participants are using the right password renewal and password setting methods. However, about 53% have not changed their password in one year, have not renewed their password since the first installation, or have not renewed for more than a year, and many participants were not able to give an answer to the question. "How often did you change your password?" By setting a strong password, there are fewer opportunities for other users, especially hackers, to guess the username/password. Strong passwords reduce security risks of data loss, data theft, and data leakage. "Clearly, cryptographically large passwords would be better" as according to Jablon [11]. A safe and strong password contains a mixture of numbers, symbols, lowercase and uppercase alphabets, and a mixture of more than 8 characters. These should not include the Personal Information (PI), such as social ID, birthday, or any words that can be found in a dictionary.

Setting a strong password by using a mixture of symbols, numbers, upper-case, and the lower-case alphabets with at least 8 characters is recommended. Password renewal is also important to ensure staff periodically change their password within a certain period, - for example, three or six months -, and systems should be in place to prevent the old password being used again. People prefer to select easy-to-remember passwords which are considered to be weak and susceptible to another type of attacks such as dictionary-attacks [17]. Strong passwords (combination of numbers, symbols, lowercase and uppercase alphabets, and a mixture of more than 8 characters) are often hard to remember [18] but the main advantage is difficult to guess by cybercriminals. A weak password offers more opportunities for the attackers to access the computer systems and strong password is considerably harder for the computer systems to be compromised and controlled by attackers.

4.11 Database Consideration

The major software program 33%) used in Tonga for the databases was Microsoft Access. Other programs, such as Oracle, Sybase, IBM DB2, SAP Sybase ASE, and Amazon's Simple DB - are not highly used in Tonga. A report from Server Watch website on August 2016 highlights some of the top databases for 2016 are as follows: Oracle Database, Microsoft SQL Server, IBM DB2, SAP Sybase ASE, Postgre SQL, Marie DB Enterprise, MySQL, and Amazon Simple DB [6]. Google, Microsoft, Amazon, and other Cloud Service Providers (CSP) provides databases and "each one of them has their own demerits and merits" [23]. The Government of Tonga should make recommendations to the appropriate organisations and CSPs to ensure that the most appropriate databases are being used. Small businesses and small organisations are likely to continue using Microsoft Access and the large organisations such as Ministry of Education and Ministry of Police are to decide the appropriate databases that suit their needs.

5 SUMMARY

Tonga's computer systems are susceptible to cybercrimes and cyberattacks. The authors have detailed recommendations about the weaknesses and areas to be strengthened in computer systems of Tonga. The tasks recommended will assist in filling some vulnerability gaps to slow down the growing number of cybercrimes in Tonga. Although many of the areas covered in the recommendations of this paper may be new to some organisations, there is a confidence by the authors that government organisations in Tonga will take heed.

6 CONCLUSION

A study of cybercrime and cybercrime awareness in Tonga in 2016 identified a number of concerns for organizations and government departments of Tonga. This paper has built on that research and recommended eleven different areas where the people of Tonga and the government of Tonga should consider implementing sustainable strategies to mitigate risks associated with cybercrimes and cyberattacks. Given the number of concerns raised in the study the researchers felt it imperative to raise the alarm, to ring the bell, to alert the people and the government of Tonga. But the rather than just raise the alarm the authors have identified specific areas they need addressing and have suggested specific recommendations in the hope that the organizations and government of Tonga can be prepared for the increasing global rise of cybercrimes and cyberattacks.

REFERENCES

[1] Abdollahzadegan, A., Hussin, C., Razak, A., Moshfegh Gohary, M., & Amini, M. (2013). The organizational critical success factors for adopting cloud computing in SMEs.

[2] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems, 25*(6), 599-616.

[3] Careers New Zealand. (2018). *Penetration Tester*. from https://www.careers.govt.nz/jobs-database/it-and-telecommunications/information-technology/penetration-tester/.

[4] Carroll, M., Van Der Merwe, A., & Kotze, P. (2011) Secure cloud computing: Benefits, risks and controls. In *Information Security South Africa (ISSA), 2011* (pp. 1-9): IEEE.

[5] Forrest, S., Hofmeyr, S. A., & Somayaji, A. (1997). Computer immunology. *Communications of the ACM, 40*(10), 88-96.

[6] Forrest Stroud. (2017). *Top 10 enterprise database systems of 2017*. from https://www.serverwatch.com/server-trends/slideshows/top-10-enterprise-database-systems-to-consider-2015.html.

[7] Hawkins, S. M., Yen, D. C., & Chou, D. C. (2000). Disaster recovery planning: a strategy for data security. *Information management & computer security, 8*(5), 222-230.

[8] Henard, F., & Leprince-Ringuet, S. (2008). The path to quality teaching in higher education. *Paris: OCED Publication.–2008*.

[9] International Underwriting Agengies Ltd. (2016). *Ten reasons to buy cyber liability insurance*. from https://www.iua.co.nz/site/iua/files/Cyber10Reasons.pdf.

[10] ISO. (2013). *International Organization for Standardization*. from http://www.iso.org/iso/iso27001

[11] Jablon, D. P. (1996). Strong password-only authenticated key exchange. *ACM SIGCOMM Computer Communication Review, 26*(5), 5-26.

[12] Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition, 37*(11), 2245-2255.

[13] Kaniva Tonga. (2016). *Tongan bank customers hit by Fiji ATM targeted scam*. from http://kanivatonga.nz/2016/03/tongan-bank-customers-hit-by-fiji-atm-targetted-scam/.

[14] Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security, 67*, 267-279.

[15] Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security, 13*(9), 2226-2239.

[16] Kulkarni, G., Gambhir, J., Patil, T., & Dongare, A. (2012) A security aspects in cloud computing. In *Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on* (pp. 547-550): IEEE.

[17] Lin, C.-L., Sun, H.-M., & Hwang, T. (2001). Attacks and solutions on strong-password authentication. *IEICE transactions on communications, 84*(9), 2622-2627.

[18] Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32-44.

[19] Margaret Rouse. (2018). *Disaster Recovery Plan*. from https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan.

[20] McDermott, J. P. (2001) Attack net penetration testing. In *Proceedings of the 2000 workshop on New security paradigms* (pp. 15-21): ACM.

[21] Ministry of Information and Communication. (2013). *Tonga conducts Cybersecurity and Cybercrime workshops*. from http://www.mic.gov.to/regional-a-workshops/4318-tonga-conducts-cybersecurity-and-cybercrime-workshops.
[22] Moia, V. H. G., & Henriques, M. A. A. A comparison of encryption tools for disk data storage from digital forensics point of view.
[23] Ramanathan, S., Goel, S., & Alagumalai, S. (2011) Comparison of cloud database: Amazon's SimpleDB and Google's Bigtable. In *Recent Trends in Information Systems (ReTIS), 2011 International Conference on* (pp. 165-168): IEEE.
[24] 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.
[25] Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011) The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122): ACM.
[26] Sedayao, J., Su, S., Ma, X., Jiang, M., & Miao, K. (2009) A simple technique for securing data at rest stored in a computing cloud. In *IEEE International Conference on Cloud Computing* (pp. 553-558): Springer.
[27] Simon Grubisic. (2009). *How ATM card skimming and PIN capturing scams work.* . from https://www.slideshare.net/worldstuff/how-to-detect-atm-card-skimming-and-pin-capturing-scams.
[28] Siuta Laulaupea'alu. (2016). *Data Security Assessment for Government Information Systems in Tonga.* . Unpublished Master Thesis, University of Waikato, Hamilton. .
[29] Telarc. (2015). *Quality*. from http://www.telarc.co.nz/services-and-standards/quality/
[30] The University of Waikato. (2017). *Ryan Ko's top five cyber safety tips*. from https://www.waikato.ac.nz/news-events/media/2017/ryan-kos-top-five-cyber-safety-tips.
[31] The University of Waikato. (2018). *Master of Cyber Security*. from http://www.waikato.ac.nz/study/qualifications/master-of-cyber-security.
[32] Tian, Z. (2014). *Digital forensics in the Cloud: encrypted data evidence tracking.* thesis, Auckland University of Technology.
[33] Yeo, J. (2013). Using penetration testing to enhance your company's security. *Computer Fraud & Security, 2013*(4), 17-20.
[34] Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems, 30*(1), 123-152.
[35] Zhu, Z. (2017). Automated Penetration Testing for PHP Web Applications.