CYBERCRIME AND ITS IMPLICATIONS TO THE PACIFIC

Glen Finau[1], Jale Samuwai[1] and Acklesh Prasad[2]

[1]The University of the South Pacific
[2]Queensland University of Technology

Introduction

Cybercrime consists of any criminal action or behaviour that is committed through the use of Information Technology. Common examples of such activities include cyber hacking, identity theft, cracking, spamming, social engineering, data tampering, online fraud, programming attacks, etc. The pervasive use of the internet clearly indicates that the impacts of cybercrime is far reaching and any one, may it be a person or an entity can be a victim of cybercriminal activities. Recently in the US, eight members of a global cybercrime ring were charged in one of the biggest ever bank heists. The cybercrime gang allegedly stole US$45 million by hacking into credit card processing firms and withdrawing money from ATMs in 27 countries (Jessica et al. 2013). An extreme example, the above case highlights how IT is changing the way crimes are being committed. No longer do criminals use masks, guns and get-a-way cars, criminals are able to commit crimes in the comfort of their homes, millions of miles from the scene of the crime and can access significant sums of money that can financially cripple organisations. The world is taking notice of this growing threat and organisations in the Pacific must also be proactive in tackling this emerging issue.

Cybercrime in the Pacific

The current IT revolution in the Pacific has provided significant opportunities but at the same time also brought about significant risks. The boom in the use of mobile computing in the Pacific has enabled the region to leap frog computer based internet connections. The Pacific has seen drastic improvements on mobile penetration rates in the past decade with countries such as Fiji, Samoa, Vanuatu and New Caledonia now enjoying a mobile penetration rate of over 80 percent (Cave 2012). Such pervasive use of mobile computing is possible through the continuous improvement of the telecommunications network from 3G to 4G standard. Internet penetration rate is still however still relatively low due to high access costs.

For businesses in the Pacific, cyber security is now a growing concern as Pacific Island Countries are becoming an integral part of the global networked economy. Pacific Island Countries are embracing the internet as a major part of their business processes. This is evident in the growing number of businesses using the internet for marketing purposes, communication and collaborations and more recently to facilitate payment transactions. Given the fragility of IT infrastructures in the Pacific, many online businesses in the Pacific island are vulnerable to cyber-attacks. Examples of which include the telephone number hijacking incident in the Cook Islands that resulted in an estimated loss of over USD$100, 000 and the two day long severe denial of service attack (DoS) in the Republic of the Marshall Islands that crippled their network (Tabureguci 2007). More recently, a failed attempt to hack the Fiji National Provident Fund prompted FNPF to strengthen their IT

security (Swami 2013). Such incidents are clear indications that cybercrimes are a real threat and need to be addressed appropriately.

Securing the business data and its infrastructure from cybercrimes should now be a top priority for most businesses. Commonly referred to as infosec (information security), such practices cover a broad range of activities from good internal control practices, system audits to investment in intelligence systems. The International Telecommunication Union (ITU) has compiled a more detailed list of recommendations and practices that businesses as well as the government should consider in ensuring IT security (Wamala 2012). It is important for businesses to understand that infosec is not a state but a journey. It is a continuous process that demands the support and the commitment of senior management and the continuous transformation and renewal of corporate culture in relation to their perspective of IT. It is critical for businesses in the Pacific to understand and appreciate this as many tend to adopt a reactive approach to IT.

Source: www.paranet.com

Government initiatives to combat cybercrime

A number of Pacific Island Countries have developed laws to deal with cybercrime and some have even implemented specific cybercrime legislation such as Tonga. Cybercrime or Internet Law in general is a complex and contentious issue. In Fiji, the government has been proactive in its attempt to protect its national IT infrastructure as well as the users from being exploited by cybercriminals. Some of these legislative initiatives include the formation of the Anti-Money Laundering guidelines, the inclusion of computer related offences in the 2009 Crime's Decree and the protection of consumer rights, the illicit use of ICT under the 2010 Commerce Decree and the current discussions for the development of a Cybercrime Legislation in Fiji . Structural initiatives include the formation of the Financial Intelligence Unit (FIU) to monitor the financial transactions in the financial industry, the setting up of a Cybercrime Unit under the Ministry of Defense, the formation of a Cybercrime Working Group and the establishment of the Pacific Computer Emergency Response Team (PacCERT) whose specific responsibilities include facilitating, coordinating and monitoring activities related to cyber security and safety and to provide fast and effective responses to cyber security incidents and threats to organisations in the Pacific.

The Role of the Accountant with respect to Cyber security

The growing threat of cybercrime globally requires all employees of an organisation to be aware of cybercrime dangers and to take appropriate measures to reduce the risk of cyber threats. Accountants especially have an important role with relation to an organisation's cyber security. Accountants are the "keepers" of their organisation's financial information assets and these are usually the information most sought after by cybercriminals. Accountants therefore must be aware of cyber threats, cyber laws and measures to reduce the risks of cyber threats in their respective organisations. Ignorance cannot and should not be an excuse for accountants. An organisation's cyber security strategy requires all employees to be trained in cyber security measures and be able to identify cyber security threats as early as possible. While the responsibility of cyber security primarily rests with an organisation's IT department, all employees play an important role in effectively implementing their organisation's cyber security plan.

Forensic accountants are also playing a major role in combatting and catching cybercriminals. Forensic accounting is a dynamic field and requires knowledge in various subjects such as accounting, law, criminology and information systems. The pervasive use of IT to commit fraud has required forensic accountants to be well versed with IT and IT-related crimes. In developed countries, audit firms have their own cyber fraud squads to investigate crimes and evaluate an organisation's security systems (Goodin 1999). Pacific Island Countries will also have to develop their national capacity of forensic accountants to fight against cybercrime.

Conclusion

This article has sought to engender a greater awareness of the growing threat of cybercrime in the Pacific. Pacific Island Governments are cognisant of cyber threats and have implemented or are in the process of developing legislations related to cybercrime. Some organisations in the Pacific as well are beginning to invest more in IT security and developing IT security strategies. Accountants are crucial in the success of these strategies as accountants are the "keepers" of financial information assets. The importance of developing forensic accountants in the Pacific has also increased as forensic accountants play an important role in the prevention, detection and enforcement of cybercrime.

REFERENCES

Cave, D. 2012. "Digital Islands: How the Pacific's ICT Revolution is Transforming the Region", Lowy Institute for International Policy, November, 1-22.

Goodin, D. 1999. "Accounting firms fight cybercrime - CNET News", Available at, http://news.cnet.com/Accounting-firms-fight-cybercrime/2100-1023_3-226713.html, [Accessed 24 May 2013]

Jessica, D., and Jim, F. 2013. "US Charges Eight in $45 Million Scheme," Available at, http://www.cnbc.com/id/100724220,[Accessed 24 May 2013]

Swami, N. 2013. "FNPF beefs up security," The Fiji Times, Monday, May 13th.

Tabureguci D.2007." *Pacific telephone number fraud victims get ITU sympathy*", Available at http://www.islandsbusiness.com/islands_business/index_dynamic/containerNameToReplace=MiddleMiddle/focusModuleID=18505/overideSkinName=issueArticle-full.tpl [Accessed 24 May 2013].

Wamala, F. 2012. "The ITU National Cybersecurity Strategy Guide", Available at, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [Accessed 24 May 2013].