CYBER SECURITY IN THE MODERN WORLD: AN ANALYSIS OF CYBER SECURITY AND LEGAL FRAMEWORK IN THREE ASIAN COUNTRIES

Rosharn Amarasinghe[1], MEP Ranmuthugala[2]
General Sir John Kotelawala Defence University, Sri Lanka
rosharn.amarasinghe@gmail.com

Abstract- The advent of information technology has resulted in advanced but virtual or cyber security threats, which decree that all nation states must safeguard their virtual boundaries and information with the same fervour as their physical boundaries. Paying attention to the multiple cyber-attacks across the world, it was identified that a strong framework to monitor hacking and other cyber threats, and well-developed mechanisms and organizations to guard national interests on multiple platforms were essential if any country is to tighten its security and ensure protection of data. This qualitative research uses secondary sources and examines three case studies from Asia and analyses the weaknesses (if any) of the government's legal framework in each country, the successes of the case study, and best practices that other countries could use from their experiences. This is balanced by the personal experiences and observations of the researcher as an employee of the industry. The legal ramifications and framework take focus in this research, and it is intended to provide a road map to governments for future cyber security investments. The paper analyses the legal frameworks in each country to better understand the necessary legal measurements to ensure cyber safety, and it offers recommendations to governments towards combatting cyber terrorism and data loss.

Keywords- Cyber security, Cyber warfare, Best practices

I. INTRODUCTION

The advent of information technology in the form of the internet has resulted in advanced but virtual or cyber security threats, which decree that all nation states must safeguard its virtual boundaries and information with the same fervour as their physical boundaries. Cyber threats are any illegal activity and malicious attempts aimed at accessing, damaging or interrupting a computer system or network (Romanosky, 2016; O'Connell, 2012; PNC, 2015). They use malware, phishing attacks, SQL injection attacks, cross-site scripting, denial of service, session hijackings, and credential reuses to attack the system (Rapid7.com, 2017). According to the Cyber Security Report (2017), in the past decade, there have been several thousand threats launched over the cyber space. In India, the first half of 2017 saw 27482 threats (Salman, 2017). In 2017 alone, global cyber security crime cost an estimated USD 1 trillion and it is expected that costs will be 6 trillion by 2021 (Forbes, 2017), which is one-third of the gross domestic product of the USA in 2015 (Trading Economics, 2017). Thus, a major threat to contemporary national security has arisen in the cyber arena motivated by financial or political goals.

Cyber threats have far-reaching consequences for both the government and private sectors. The attacks on LinkedIn (Wood, 2016), My Space (Francis, 2017) and Tumbler (Hern, 2016) in the period 2012-2016, as well as the softwares WannaCry (Symantec Security Response Team, 2017) and Petya (Solon and Hern, 2017) have elaborately demonstrated the devastating legal and economic consequences and backlash of an attack – whether perpetrated maliciously by an outside threat or through the inadvertent actions of an insider. Given the global reach of these attacks, the global banking industry invests heavily in solutions to combat such threats.

According to Cassim (2017), currently the most encountered malware programs are "Gamarue, a malicious computer worm that is commonly distributed via exploit kits and social engineering; and Skeeyah and Peals, which are Trojans that try to look innocent to convince users to install them." These malware programs operate by stealing information (credit card information, passwords, birthdate information, etc.), downloading other malware onto the computer it is currently inhabiting, or by providing access to a hacker so that the hacker can access the information and systems of the computer. The solution software industry is expanding rapidly, offering solutions such as cloud-based, application-based and physical resources (software and hardware) to prevent, counter, and combat attacks from both outside and inside.

Governments face threats far in excess of what private companies do and they run a larger risk in not updating their security measures. The recent allegations over Russian influence in the US presidential elections (The Sydney Morning Herald, 2018) are a case in point of the need for increased government vigilance on all fronts, especially the cyber space. If a country is to tighten its security and ensure protection of data, it was identified that a strong framework to monitor hacking and other cyber threats were essential, along with well-developed mechanisms and organizations to guard national interests on multiple platforms.

A. Sri Lanka's History of Cyber Threats

The country has weathered many threats, especially with organised groups hacking into government networks in the mid-1990s. During the height of the war, the LTTE released many high-impact pictures of murdered civilians and bombed locations to tarnish the Sri Lankan brand. In recent times, revenue has been lost due to data breaches and system downtime. Given that an increased overall attack pattern on government and critical services can be observed, Sri Lanka must understand the interconnectedness of national security and cyber security. Sri Lanka lags in its approach to and understanding of cyber security, a situation that needs urgent rectifying, given the continued as well as recent attacks on both governmental and corporate entities.

B. Bangladesh

A major breach of security occurred in Bangladesh, which shone a light on the vulnerabilities that many developing nations labour under. Cassim (2016) reports that "more vulnerable countries saw over 40% computers hit by malicious software compared to the world average of 21%." The modern-day, digital bank robbery in Bangladesh had repercussions around the world, linking Asia and Europe in its reach.

C. Singapore

The developed country addressed in this research, Singapore provides the best practices for others around the world to follow. With a comprehensive legal framework put in place following the attack, Singapore provides safety not only to its citizens but also to other countries.

II. METHODOLOGY

This is a desk research looking into the threats faced by the governments of Sri Lanka, Bangladesh, and Singapore, with the view of understanding the larger ramifications of being vulnerable in the cyber space. The research aims primarily to bring to the fore the need for cyber security management and secondarily to provide examples of best practices from the region for use by governments. The paper answers the following research questions: Firstly, what legal framework exists for cyber security threat management in each country? Secondly, what are the threats that these countries face in economic, political, and diplomatic spheres due to cyber threats? Finally, what are the current best practices in combating cyber terrorism? Do these countries use them and if not, why do they not?

III. RESULTS

A. Sri Lanka

'Lanka Clear' is the central cheque clearing agency in Sri Lanka, handling all financial transactions in terms of cheque management for all banks and financial institutes. It comprises of members of all banks as the management body and regulates the industry for payment management in cheque mediums and is a highly regulated agency governed by the Central Bank directives that cover cyber security, governance and information management (Lanka Clear, 2018). In late 2000s, a focused attack was executed on the web applications and website of Lanka Clear due to un-deployed web security protocols (although mandated by the Central Bank), where the website was compromised, and hackers commissioned by the LTTE working out of India gained access and administrator rights to the website. Subsequently, disturbing images of murdered children and war-torn areas were published across the website with links and screen captures sent to war crimes units. The purpose was to pressurize the Sri Lankan government into entering a ceasefire agreement as the LTTE battle lines had fallen in most locations. Due to the lack of a strong web security and governance cycle, Sri Lanka suffered a substantial loss in terms of trust and financial stability within the region. As Lanka Clear is the only cheque processing facility in the country, regional financial organizations and trade partners expressed concern in terms of the compromise of critical data pertaining to transactions carried out with Sri Lanka as well as the safety of data within Lanka Clear.

Cyber-attacks have also caused regional instability by affecting several countries interconnected in cross-border financial transactions. The Bangladesh Bank attack is a strong example of the financial and reputation loss incurred due to cyber-crime (Khandelwal, 2016b). The banking standards for interbank financial transactions is governed by SWIFT policies. The Bangladeshi Central bank was operating their core services without the implementation of a core firewall within their network (Kumar, 2016; Khandelwal, 2016). The functionality of the said device is to monitor all information transferred in and out of the central bank for irregularities. In May 2015, four bank accounts were opened in the Philippines Bank that were used in 2016 to instigate a cyber-attack amounting to an estimated US$1 billion (Schwartz, 2016). The attack was carried out on the same day in February 2016 attacking the core digital cash transfer system of the Bangladeshi Central Bank, due to the lack of a core firewall to protect the network. Since the attack was not reported in depth, some information is based on available estimations. The attack provided the hackers with access to the core server that was used to execute the said transactions. The destination countries were Sri Lanka and Philippines where 35 payment instructions worth $81 million (Gopalakrishnan and Mogato, 2016) were issued from the Federal Reserve Bank. The attack was successfully carried out with only the final few transactions being rejected due to a spelling error in the issued payment advice, which alerted the Deutsche Bank who flagged it as suspicious. A total of $81 million was withdrawn during February 2016 leading to one of the largest overhauls within one single country in the SAARC region.

B. Singapore

In January 2013, a global hacking organization, Anonymous announced war against the Singaporean government (Lee, 2013). The reason highlighted was the $130 million investment by the Singaporean government to counter cyber-threat and hacking within the island nation. Anonymous claimed that the hacks they carry out is for ethical purposes to highlight corruption and threats globally and that if a country is investing against their interests, it would launch a cyber war against such opponents. Accordingly, in mid-2013, attacks were launched against several government institutes as well as the government-managed newspaper 'Strait Times' or ST (Lee, 2013). The reason for the attack on ST was that a journalist within the newspaper had changed anonymous quotes from launching a war against the "Singaporean government" to "Singapore", purposely focusing on an attack on the country rather than on the government. An Anonymous hacker named "Messiah" claimed responsibility for the attack. In addition to the attacks against the government, Anonymous instigated an attack against Standard Chartered Bank, attacking servers held at Fuji Xerox Singapore. It was noted that data belonging to over 647 high net individuals were stolen and the same hacker was linked to the attack.

As a result of the attacks and focused hacking attempts, the Singaporean government engaged in an Asia Pacific- level Cyber Threat Readiness Agreement with Australia. This provided a strong platform on which to engage the resources of both countries in fighting cyber threats via a regional Security Operations Centre or SOC, which is utilized to analyse data from each country's critical systems to ensure that irregular activities do not take place. The systems provide a proactive mechanism to counter cyber threats and attacks. In November 2017, both countries announced that the cyber threat platform in place had yielded positive results showcasing the possibility of managing threats via regional cooperation.

IV. DISCUSSION

A. Sri Lanka

In the case of 'Lanka Clear, there was a problem with sensitive data because Lanka Clear is the only cheque processing facility in the country. This fact has led to an expressing of concern by concerned parties such as regional financial organizations and trade partners in relation to both the safety of sensitive data and the safety of working with Lanka Clear. As a remedial mechanism, a web security appliance was launched, but this proved to be a reactive action as the damage to the country was already done. Lanka Clear is still used as a focus point of government-based financial processing and this provides a strong platform to increase awareness within the government sector on cyber security protocol. At present, Lanka Clear has transformed itself into a highly compliant entity engaging best-of-breed cyber security products to battle continuous attacks to the network. Although the entity itself is now compliant, Sri Lanka is yet to create a strong cyber security policy in terms of law making and enforcement as well as management of data or information shared amongst government bodies and third-party organizations. Thus, it is possible to see that the repercussions of a cyber-attack extend far beyond the immediate time frame. Companies such as Lanka Clear need to be vigilant from this point forward to ensure both that a similar incident does not happen and that its reputation is cleared.

B. Bangladesh

Following the massive heist, Bangladeshi banks commenced heavy investments into security technology and services. In addition, the government set strong regulations via the Central Bank to govern the process of data processing and management. As noticed within the case study, regional effects of cyber-attacks spread beyond a nation's boundaries leading to damaged trust that can affect a country's economy, development and growth. Bangladesh as a country had not focused heavily on cyber security readiness and investment as it had not faced traditional threats within this sphere. On realization of the attacks and the damage it caused to both the country as well as the people, heavy investments were made within this domain. The central bank of each country governs most of the data management regulations and this was noted to be lacking within the country. In addition to the following, a strict national guideline was initiated for cyber security threat identification, management and resolution. This was deemed to be of crucial importance as it engaged the whole country, on the matter of readiness for the expected non-traditional wars in future.

C. Best practices – Singapore

The island nation is positioned with a strong regional ability to combat cyber-threats due to the knowledge hub and infrastructure built around cyber-threat defence mechanisms. Due to the organized attacks launched against the country, investments on data management, identification, monitoring and threat response have yielded strong outcomes within the cyber-threat mitigation domain. As most hack attempts remain undetected for months, the Singaporean government noted that successfully managing cyber-crime and threats needs a strong mechanism for detection. Thus, the government's investment into a regional Security Operations Centre has provided a working platform and model for other countries to follow. According to several cyber groups that rank countries based on cyber threat readiness, Singapore has featured as a strong global force in combating cyber-threats.

An analysis into the Singaporean success story shows three major components that contributed to building a strong nation geared for cyber war: Information dissemination – Sharing of information and best practices have been a key feature (Koh, 2017). Singaporean governmental and private institutes invest heavily in training and development as well as knowledge sharing across departments and groups. It was noted that most attacks no longer arise externally but internally due to accidental malware and virus outbreaks. Information dissemination assists in combating such threats as all stakeholders are regularly updated on current threats in each organization.

The second component is threat detection/response. Each organization's ability to detect anomalies in the network and mitigate accordingly has been a key differentiator in the level and severity of data loss. As most government organizations in Singapore follow a fixed standard to protect information, this process becomes easier. Countries such as Bangladesh and Sri Lanka execute ad hoc protection mechanisms that are not standardized across entities. Due to these reasons, when attacks and threats successfully enter the institutes, it provides a platform to move into other organizations through communication channels. Singapore maintains strict mechanisms to detect threats via continuous proactive software solutions. In addition, the central bank and other security-related agencies provide a guideline on best practices to mitigate risks and threats from cyber-attacks. A strong detection and response mechanism is essential and recommended for all countries and organizations to maintain a sustainable cyber-attack readiness framework.

Thirdly, regional cooperation ensures Singapore maintains a strong data sharing policy, for information and threat responses. Singapore leads the region in training and development. It is noted that whilst countries such as the USA and China maintain strict policies on sharing information, Singapore embraces an open culture of learning and sharing of past experiences and threat vectors with all entities. This provides a faster learning curve for developing countries as well as gaining diplomatic ground for other trade and knowledge-based ventures. Regional cooperation extends to assisting government entities fine tune their data protection policies, as seen in Australia as well as Japan. Singapore maintains a threat-response mechanism that provides regional data to the government as per agreements signed between nations as well as security governance entities. The mechanisms adopted by Singapore promote sustainable growth of cyber defence policies. It must be noted that cyber warfare is not restricted to a single country and information facilitation strengthens global cyber protection, which mutually benefits nations across the map.

D. Legal Ramifications

Laws governing countries can and must protect the citizens and their data. What laws exist in the three selected countries to protect from cyber-threats? Sri Lanka has passed many laws impacting on and affecting the cyber security domain of Sri Lanka (Kotelawala Defence University, n.d.), including the following:

i. Information and Communication Technology Act (No.27 of 2003) - This Act aims to improve Information and Communication Technology and solve conflicts. In addition, it aims to introduce and implement a national policy on ICT.

ii. Evidence (Special Provisions) (Act No.14 of 1995)

iii. Intellectual Property Act (No. 36 of 2003 (Sections related to Copyright) - For copyright infringement matters

iv. Electronic Transactions Act (No. 19 of 2006) for matters pertaining to the creation and exchange of data messages

   i. electronic documents

   ii. electronic records

   iii. other electronic communication

v. Computer Crimes Act (No. 24 of 2007) - This Act deals with the prevention and punishment of computer-related crime, thus hacking and cyber-crimes are included in this. The Penal Code is undergoing changes to take these new developments into consideration.

vi. Payment and Settlement Systems Act (No. 28 of 2005)

vii. Payment Devices Frauds Act (No.30 of 2006)

The Computer Crimes Act, in sections 3 to 10 (cited in Jayasekara & Rupasinghe, 2015), states as follows:

i. The illustrations given in the Act states that for any unauthorized modification or damage or potential damage to take place, any one of the following should occur

ii. Impairing the operation of any computer, computer system or the reliability of any data or information held in any computer;

iii. Destroying, deleting or corrupting or adding, moving or altering any information held in any computer;

iv. Making use of a computer service involving computer time and data processing for the storage or retrieval of data;

v. Introducing a computer program that will have the effect of malfunctioning of a computer or falsifies the data or any information held in any computer or computer system (e.g. viruses, worms, etc.).

At present, the cyber-crimes division is engaged in locating perpetrators. Added resources such as a military unit can bring rapid justice. However, a problem arises in dealing with non-citizens such as the Pakistani hacker, at which point Sri Lanka must rely on international law.

However, while a legal framework exists in Sri Lanka, it is not currently viewed as strong, as experts have deemed that the infrastructure within the government sector is not equipped to handle strict regulatory processes. Many organizations such as ICTA and Sri Lanka Computer Society have engaged the government on the matter considering increasing readiness for cyber threats and management. As a region, SAARC has investigated the possibilities of establishing a common platform for cyber readiness such as the APAC alliance set up between Singapore and Australia. This allows information sharing as well as best practice application, knowledge sharing and management of critical situations. It has been noted by both the Singaporean and Australian governments that resource sharing in terms of cyber security management and mitigation has been noted to be effective as each country faces both common and unique threats. The pooling of resources provides a stronger battle front for governments to engage and mitigate global cyber security attackers focusing on APAC. Singapore has been focusing on regional standard establishment and it is expected that over the next three to four years Sri Lanka, India and other nations will engage on a common framework for the region. Bangladesh, Sri Lanka and other countries can benefit from benchmarking Singapore's legal frameworks as the maturity of the protocols in place are high. In addition to the mentioned protocols, a structured approach is utilized in adhering to international standards in processing critical information and risks.

Singapore follows global security standards such as NIST that provides a framework for legal processes and the management of task-based execution. Legal frameworks in IT security are applicable to processes, people, and security solutions based on the area of application. At present, since most countries do not adopt a dedicated legal framework, this has led to many gaps in the overall policy. Analysis of events and audit trails is the only method available for countries such as Sri Lanka and Bangladesh as the investments into automated policy-based monitoring mechanisms are not in place. The private sector has not contributed significantly to a national security policy as the entities focus on internal security management rather than a country-wide security posture. The private sector maintains The private sector maintains highly skilled security workforces that can contribute significantly both in terms of creating sustainable policies and managing future risks through awareness creation and knowledge sharing. Bangladesh and Maldives rely on Sri Lanka's CERT team, as they have not invested in retaining skilled professionals within the cyber security and IT domains. Thus, another gap exists to leverage on Singapore and Sri Lanka's skilled workforce for IT security enablement among developing countries and Sri Lanka has the potential to become a regional thought leader within the security domain given the many IT professionals within the local market. However, the lack of information sharing has become a primary concern. Each government department functions in isolation with staff and managers unwilling to share data and information with other government bodies. The lack of education in cyber security is a major barrier as many senior staff members have low computer literacy rates. Propagation of viruses and hackers within the network is always higher when staff are not trained to highlight and identify particular risks. Currently the global standard for cyber security life cycle management is the NIST framework issued by the US government and the framework is adopted by most security-focused entities. The framework covers data management, processing as well as deletion, ensuring that data removed cannot be recovered and used. In addition to the NIST framework, PCIDSS and ISO27001 frameworks are used for process-based IT security standards. These policies focus on how credit card information is managed and how an organization addresses various aspects of data privacy and security. Sri Lanka uses a combination of PCIDSS and ISO27001 for a few government entities but has not standardized across all government agencies leading to gaps in data processing and security. PCIDSS is applied to most of the government banks and central agencies for financial services. Given the high adoption rate in private enterprises, ISO27001 is mainly used by these enterprises. Compliance is easier when standard mandates are applied to all entities. As Sri Lanka is still in the process of adopting core security principals within the government sector, a few years will be required to ensure that standards are complied with.

V. CONCLUSION

Government investment within the cyber security domain has increased recently but a large gap exists in the creation of a sustainable IT-based hub in Sri Lanka. The government has not implemented clear procedures to address the growing demand for secure transactions. Although basic legal frameworks exist within the cyber-crime and data management arena, a significant gap exists in comprehensive IT legislation. Additionally, the lack of cyber security lawyers in Sri Lanka has contributed to delays in establishing clear protocol and guidelines.

Conversely, the private sector maintains senior resources within the cyber security domain specializing in data management standards, auditing and compliance. Each private institute focuses on internal risks and compliances rather than an industry-based mechanism to assist other organizations. Thus, exists data sharing and transfer between organizations is inefficient or non-existent. The private sector is poised to assist the war against cyber terrorism provided that knowledge and information sharing is facilitated between organizations. Currently telecommunication companies and banks command strong resources to assist in their security operations and these resources can be utilized to increase the overall security governance and compliance posture of Sri Lanka. As most core economic processes such as banking, stock exchange and management of funds are digital, the risk of cyber threats is high. Due to the risks created by a digital platform, a comprehensive security mechanism with failover options is required to be safe from cyber-attacks. As diplomacy plays a crucial role in managing relationships with regional entities, it is noted that a cyber security dialog or forum would immensely assist Sri Lanka's cyber security readiness campaign.

In examining the need for cyber security, it is evident that all governments must invest heavily into setting up systems that will effectively and efficiently guard the information and users of the country. The government cannot detach itself from the network usage of the individual and must ensure that the user is consistently protected. Administrators must be competent and invested authorities, rather than students of networking or website development. All companies and entities must understand that their internet presence is not only to send messages out unilaterally to public but to also safeguard the interests of their clients. Till this is understood, no amount of work will be enough to keep the country and its information safe. Entities must invest in heavy-duty, effective mechanisms that are both up-to-date and state-of-the-art, to ensure that all ransom ware and malware are detected in a timely fashion and neutralized before they cause harm. Keeping in mind that it is possible for hackers to enter the system even 18 months prior to their malicious actions, it is necessary to invest in systems that will keep abreast of the administrative accounts (to shut down any that are not in use or are unnecessarily created). It is in the interests of the government to create a nexus between industry experts, companies in the industry, and the government. The industry experts should be called on to lead the change in mechanism as well as to train and teach. The companies should ensure, and be allowed and encouraged to ensure, that all computer networks are protected, and that hacking and other security threats - including both insider and outsider threats – are minimized. A national policy must be created that leaves room for future advancements while acting as a barrier to outside threats. This policy can be the guide for instances of a threat. The policy should help make existing laws more effective and realistic, and universally followed. The government must oversee the companies through regulations since deregulated businesses cause more damage than regulated companies. Finally, the IT security sector in the industry must be allowed to bloom, with the government taking necessary action to nurture it. The emphasis should be on increasing the capacity and knowledge of the sector so that it is able to handle threats without needing to resort to or depend on the government's intervention. Additionally, they must be given adequate resources (monetary, physical, intellectual, etc.) to ensure that they can carry out their work without impediment.

VI. REFERENCES

Cassim, N. (2016). Sri Lanka among top 10 countries in Asia facing threats to cyber security. Ft.lk. Retrieved 4 November 2017, from http://www.ft.lk/article/546719/Sri-Lanka-among-top-10-countries-in-Asia-facing-threats-to-cyber-security

Cyber Security Report. (2017). Telstra Cyber Security Report 2017. Retrieved 9 October 2017, from https://www.telstraglobal.com/images/assets/insights/resourc es/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdfForbes. (2017).

The True Cost of Cyber Crime for Business. Forbes.com. Retrieved 7 December 2017, from https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#f46680749476

Francis, R. (2017). MySpace becomes every hackers' space with top breach in 2016, report says. CSO Online. Retrieved 7 December 2017, from https://www.csoonline.com/article/3166846/data-breach/myspace-becomes-every-hackers-space-with-top- breach-in-2016-report-says.html

Gopalakrishnan, R. and Mogato, M. (2016) Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. Reuters.com. Retrieved from https://www.reuters.com/article/us-cyber-heist- philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH

Hern, A. (2016). More than 65m Tumblr emails for sale on the darknet. The Guardian. Retrieved 5 December 2017, from https://www.theguardian.com/technology/2016/may/31/tumb lr-emails-for-sale-darknet-65-million-hack-passwords

Jayasekara, D. and Rupasinghe, W. (2015) Cyber Crime in Sri Lanka. Retrieved from https://www.researchgate.net/publication/294725446_Cyber- Crime_in_Sri_Lanka

Khandelwal, S. (2016). Here's How Hackers Stole $80 Million from Bangladesh Bank. The Hacker News. Retrieved 22 October 2017, from https://thehackernews.com/2016/03/bank-hacking- malware.html

Khandelwal, S. (2016b). Second Bank hit by Malware attack similar to $81 Million Bangladesh Heist. The Hacker News. Retrieved 22 October 2017, from https://thehackernews.com/2016/05/swift-bank-hack.html

Koh, D. (2017). PPDC launches new initiatives to continue its effort towards developing a trusted data ecosystem in Singapore. Open Gov. Retrieved from https://www.opengovasia.com/articles/7851-pdpc-launches-new-initiatives-to-continue-its-efforts-towards-developing-a- trusted-data-ecosystem-in-singapore

Kotelawala Defence University (n.d.) Cyber Terrorism: Is Sri Lanka Ready? Retrieved from http://www.kdu.ac.lk/faulty-of- defence-and-stratergic- studies/images/Cyber%20Terrorism;%20Is%20 Sri%20Lanka%20 Ready.pdf

Kumar, M. (2016). Bank with No Firewall. That's How Hackers Managed to Steal $80 Million. The Hacker News. Retrieved 22 October 2017, from https://thehackernews.com/2016/04/bank-firewall- security.html Lanka Clear (2018) Retrieved from http://www.lankaclear.com/

Lee, T. (2013) 'Anonymous' hackers threaten war with Singapore government. Tech in Asia. Retrieved from https://www.techinasia.com/youtube-anonymous-hacker- group-threatens-war-singapore-govt-video-removed-viral

O'Connell, M. E. (2012) Cyber Security without Cyber

War, Journal of Conflict and Security Law, Volume 17, Issue 2, 1, Pages 187–209, https://doi.org/10.1093/jcsl/krs017

PNC. Internal Threats to Your Company's Cyber Security. Pnc.com. Retrieved 5 December 2017, from https://www.pnc.com/content/dam/pnc- ideas/articles/CIB_ENT_PDF_1115-092-199724- CIB_FPS_OctArticles_CyberSecurity_rev1.pdf

Rapid7.com. (2017). Common Types of Cybersecurity Attacks: A look inside the attacker's toolkit. Retrieved 9 October 2017, from https://www.rapid7.com/fundamentals/types-of-attacks/

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. Retrieved from http://dx.doi.org/10.1093/cybsec/tyw001

Salman, S. (2017). 27,482 cyber security threat incidents in India till June 2017: CERT-In - MediaNama. MediaNama. Retrieved 6 December 2017, from https://www.medianama.com/2017/07/223-india-witnessed- 27482-cyber-security-threat/

Schwartz, M. J. (2016) Bangladesh Bank Attackers Hacked SWIFT Software Information Security Media Group. Retrieved from https://www.bankinfosecurity.com/report-swift-hacked- by-bangladesh-bank-attackers-a-9061

Solon, O., & Hern, A. (2017). 'Petya' ransomware attack: what is it and how can it be stopped?. The Guardian. Retrieved 11 November 2017, from https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

Symantec Security Response Team. (2017). What you need to know about the WannaCry Ransomware. Symantec.com.

Retrieved 13 December 2017, from https://www.symantec.com/blogs/threat- intelligence/wannacry-ransomware-attack

The Sydney Morning Herald (2018) Russia ran US election interference with no Trump collusion, panel finds. Retrieved from https://www.smh.com.au/world/north-america/russia- ran-us-election-interference-with-no-trump-collusion-panel- finds-20180428-p4zc5v.html

Trading Economics. (2017). United States GDP | 1960-2017 | Data | Chart | Calendar | Forecast |

News. Tradingeconomics.com. Retrieved 6 December 2017, from https://tradingeconomics.com/united-states/gdp

Wood, T. (2016). The LinkedIn Hack: Understanding Why It Was So Easy to Crack the Passwords. LinkedIn.com. Retrieved from https://www.linkedin.com/pulse/linkedin-hack-understanding- why-so-easy-crack-tyler-cohen-wood/

BIOGRAPHIES OF AUTHORS

Rosharn Amarasinghe is currently enrolled in the PhD program at the Kotelawala Defence University. He holds a Master of Business Administration from Cardiff Metropolitan University, a Master of Science degree in Strategic Marketing from AEU, and a Bachelor of Engineering in Electrical and Electronics Engineering from the University of Northumbria at Newcastle .In addition, he holds a Postgraduate Diploma from the Bandaranaike International Diplomatic Training Institute. He is a Business Consultant at eSec Forte Technologies India and Director – Business Development at Dynatech International. He has over nine years of experience in strategic marketing and business development within the IT sector and operates as an external consultant to several start up tech companies.

Madara Ranmuthugala is currently enrolled in the PhD program at the Kotelawala Defence University. She holds a Master of Science in Development Studies and a Bachelor of Arts (honors) in English (2nd lower) from the University of Colombo as well as a Bachelor of Arts (general) (2nd lower) from the Open University of Sri Lanka. In addition, she holds a Postgraduate Diploma in Diplomacy and World Affairs (Merit) and a Diploma in Diplomacy and World Affairs (Merit) from the Bandaranaike International Diplomatic Training Institute. She is a consultant – content strategy for a host of corporate companies and individuals. Additionally, she was the Associate Editor of the International Journal of Humanities and Social Sciences by the Al Mustafa International University.