Challenges in Business Information Systems: General Policy and Marketing Implications for Cyber Security for Businesses in Developing Countries

Rafia Naz and Eric Groves, National University of Samoa

Abstract

In this digital era where businesses in developing countries are operating in a digital environment, cyber security for businesses is a sphere that is advancing extensively. To curtail the effects from cyber security, it is important that across the different businesses and countries a multi-faceted risk mitigation strategy be implemented. Therefore, this research seeks to fundamentally outline the significance of dealing with these issues effectively. This research identifies the information system and cyber security challenges for businesses in developing countries such as network security, data breach, and policy monitoring and suggests the general marketing and policy implications.

Keywords: *Business, Information Systems, Cyber security, Policy, Developing countries*

Introduction

Business information systems around the world are increasingly dependent on cyber space and utilising that space for digitally connecting with actors within and outside of the business corporation. This is increasingly evident in the South Pacific region with a high level of digital transitions and transformations occurring at the business level (Cave, 2012). However, the infrastructure used to connect and the actual engagement on the cyber platform poses additional cyber risks which are seen as an issue of executive security. This is why cybercrime is a budding concern for businesses in developing countries (Baur-Yazbeck, 2018). Developing countries are hugely reliant on consistent and secure cyberspace, however this does not equal with that of the developed countries. Due to this heavy reliance, there are inherent susceptibilities and prospects which place their critical organisations susceptible to cyber exploitation (Zareen, Monis, Muhammad and Khalid, 2013). As a result, cyber security has become a global phenomenon (Das, Saju, and Gupta, 2020). Various Governments and businesses are instituting measures in order to avert these cybercrimes. Despite numerous measures, cyber security is still a very big concern for many businesses and developing countries alike (Chang and Coppel, 2020). This is because cyber security extortions and threats are an ever-increasing risk with more businesses falling as victims to cybercrime (Jbair, 2020). These threats have escalated cybercrime which is an extravagant form of crime in the real world today (Kayser, Ellen and Cadigan, 2019-20). The snowballing threats against businesses and critical infrastructure continue to heighten the need to advance the defence and resilience of organisations (Harry, 2020). Data analytics in this regard for network intrusion detection is pertinent (Lidong and Randy, 2020). It is also imperative to train employees not only to recognise cyber threats but also to communicate back what seems doubtful (Dudley, 2020). The dire need for prompt notification by attentive users can permit businesses to respond to threats quicker, reducing dwelling time and shielding networks. One of the significant lessons emanating from the scholarly work of Chang and Coppel (2020) has elucidated that it is vital to comprehend internet access and usage to be able to identify the level of threat. Scholars have stressed on the importance of cyber security education as well (Chang and Coppel, 2020; Kortjan and Solms, 2013; Kumar, 2020). Bharara (2013) and Lee (2013) stress on the need for protecting cyber citizens and improving cyber security. Thus, this necessitates development of cyber security policies and in this regard, developing countries are in the process of crafting their own cyber security policies and agendas, and these developing nations heavily depend on the lessons learnt from their developed country counterparts (Ellefsen, 2014). Thus, the next part of this paper discusses the Information System and Cyber Security Challenges for Businesses in Developing Countries.

Information System and Cyber Security Challenges for Businesses in Developing Countries

Information system and cyber security challenges vary across different businesses and countries. Although cyber security is a growing worldwide problem, it seems to place more stress on developing businesses and countries. Vazzana (2019) suggests that addressing gaps in information systems and cyber security should no longer be a major first world problem. Adhikari (2016) identifies the below list of cyber security obstacles faced by developing and least developed countries:

- Lack of cyber security strategies/policies and legal and regulatory framework
- Inadequate fund allocation to cyber security ecosystems
- Lack of information security awareness and persistent information security culture
- Inadequate standards and maturity models for cyber security
- Lack of a Child Online Protection Framework
- Lack of necessary knowledge, information security professionals and skills within government body
- Lack of specific sector policies, e.g., education
- Resistance to change, especially in the public sector
- Reliance on imported hardware and software
- Lack of sector-specific research and development (R&D) programs/projects, especially in education
- Lack of appropriate national and global organisational structure to deal with cyber incidents

From the above list, this research identifies three main challenges for businesses in developing countries.

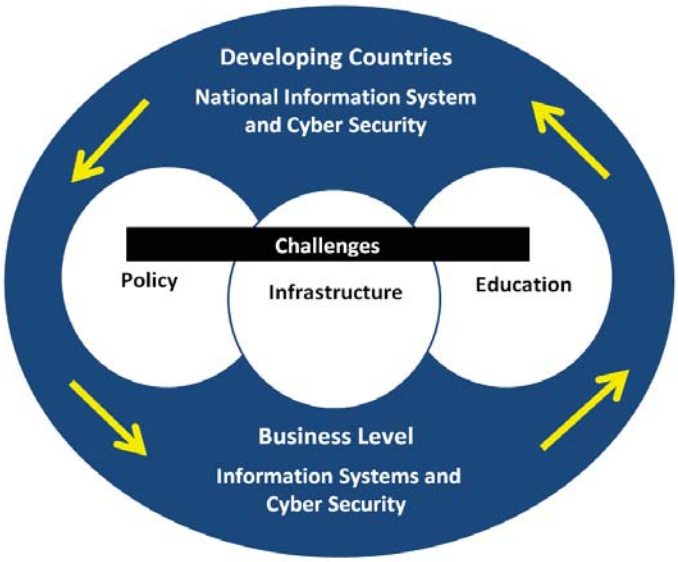
Information system and cyber security challenges are more significant for developing countries such as Samoa. This is quite obvious for reasons linked to resource constraints. Information and Communication Technology (ICT) infrastructure in particular makes all the difference in the strength and sustainability of information systems and cyber security for developing countries. The ICT infrastructures of businesses depend on the ICT infrastructure of the state or nation they are based in (Tagert, 2010). This is a major challenge because businesses based in developing countries are limited to the ICT infrastructure of the country. This means that the cyber security infrastructure for a business or corporation based in Samoa can only be as good as the cyber security infrastructure of Samoa (MCIT, 2016). This does not necessarily mean that information systems and cyber security is a dead-end. The infrastructure only limits the physical architecture and bandwidth available to the business. Electronic components such as software's and other mitigating measures like limiting access to various sites and policy enforcement are reasonable alternatives around the limited infrastructure (Muller, 2015). This alternative has been proven to be effective with several cases of accounting businesses successfully combating cybercrime (Goodin, 2002).

The second major challenge in information systems and cyber security in developing countries is education. This is both in terms of formal education and general awareness. Developing countries often have gaps in the basic computing education in the primary and secondary levels. Basic computing knowledge such as knowing how to identify spam, malware and suspicious sites and mail seem to be absent (Muller, 2015). Basic skills on how to identify the difference between legitimate and non-legitimate sources are also lacking. Students' not knowing how to identify potential security risks and basic fact from fiction on the internet is a problem that has growing consequences worldwide. Addressing these education gaps at tertiary level is far too late a step as it does not capture the students that do not continue to tertiary level or drop out at secondary level. These gaps in the education system ultimately affect the business community. Outside of formal education, general awareness is also a challenge when faced with resistance (Muller, 2015). This is predominately within

businesses and corporations that have an aging workforce not flexible to new technologies and change (Adhikari, 2016).

The third and final challenge for information systems and cyber security is the national policy and legislation. Nationally within Samoa, this is being addressed through the 'Samoa National Cyber Security Strategy 2016-2021' which targets the strengthening of national cyber security networks through its five (5) goals and strategies: (1) Develop necessary organisational structures with a focus on utilising existing structures in Samoa as well as in the region; (2) Establish relevant Technical Measure (Entities and Standards) to eliminate Cyber Threats and Attacks, Enhance cyber security and promote cyber security; and (3) Strengthen the legal framework to meet highest regional and international standards with regard to protection of fundamental rights as well as criminalization, investigation, electronic evidence and international cooperation; (4) Build digital citizens capacity, Raising awareness and attaining resources to enhance cyber security, Combat Cybercrime activities and promote Cyber safety to the highest levels; and lastly (5) Cooperation; Responding to the global nature of cyber security threats and attacks through a multi-stakeholders approach and strengthening local and global partnerships (MCIT, 2016). The five (5) goals and the strategies identified in the Samoa National Cyber Security Strategy 2016-2021 pinpoint and address the challenges listed by Adhikari (2016). Strategically Samoa is heading in the right direction in terms of policy although efforts must be prepared to make sure that it is reflected at institutional levels of businesses. Legislation challenges in developing countries in the South Pacific are becoming more evident with a growing number of businesses falling victims to cybercrime (Finau et al, 2013). Figure 1 below demonstrates the challenges and the relationship between the national and business information systems and cyber security levels:

Figure 6: Cyber Security Challenges



Methodology

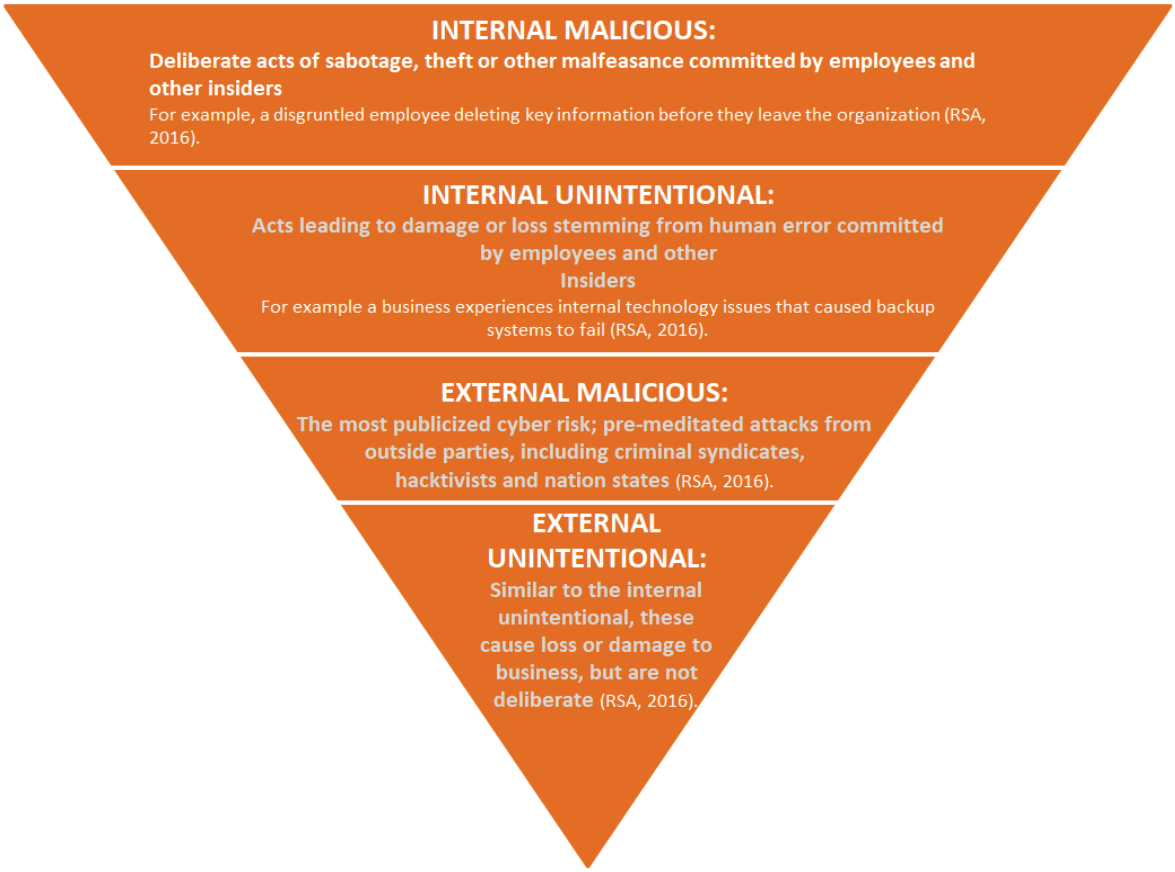
This research has undertaken a secondary based approach. Primary data has not been collected.

General Policy and Marketing Implications for Businesses in Developing Countries

In terms of general policy for businesses in developing countries, the following recommendations are made:

1. Businesses to deploy a proper cyber security risk assessment which is prominent. Risk management is not an easy task and finding efficacious mitigating measures is not as straightforward as it seems. Given that cyber threats keeps escalating together with the sophistication of the threats, standard risk analysis methodologies can help to score the cyber risk and to place it in the risk tolerance matrix. The below cyber security risk tolerance matrix identifies four (4) levels of information system and cyber security threats:

Figure 7: Business Information System Cyber Security Matrix



2. The general identification of threats in the above matrix will allow the businesses to figure out tolerable outrage for critical processes and if extra measures are needed. Cyber risk is also evaluated to classify threats to precedence systems and assets that are elected because it is too expensive to shield everything equally. If business ICT professionals align better and work together with management, then redundancies can be eradicated and the business data can be protected.

3. Governance is also an imperative theme in cyber security, as it pronounces the policies and processes which regulate how the business identifies, averts, and retorts to cyber incidents. Thus, implementing the right mix of people, policy, architecture, training and technology can enable the business to be more secure. As part of the information security governance and risk management, explicitly identifying the information assets and the advance, certification, execution and apprising of policies, standards, procedures and guidelines to achieve confidentiality, integrity and availability is critical. Information security governance should ensure that the business has the precise information structure, direction, and leadership. By this, governance implies that the proper administrative controls to mitigate risk are intact. This includes regular information system

risk analysis which benefits by providing secure governance that in turn permits proper administration of records.

Governance structures of businesses are vital as it determines who sits on the table in terms of managing cyber risks. Governance in response to business information systems and cyber security must have a good balance between business managerial and technical expertise. The below figure attempts to be a starting point to demonstrated this balance in the information system governance of business organisations:

Figure 8: Business Information Security Governance

Image: RSA, 2016

Each group identified above needs to be part of the risk management conservation. It is significant that the groups understand how each individual influences and impacts the business information system and cyber security position (RSA, 2016). This creates a better team environment within the business organisation.

2. Network security is very significant part of policy to securing the business computer network from intruders, as well as keeping software and devices free of threats. This requires businesses to practice access control, and regularly procure antivirus software, anti-malware software, application security, data analytics, behavioral analytics, data loss prevention, email security, firewalls, and distributed denial of service prevention as measures to prevent threats.

3. Management policy for the different types of businesses pertaining to assurance to data and information security is critical as well. For this, in most businesses, user activity profiles are generated for anomaly detection. This includes gathering data attribution, and context information such as user location which is pertinent for tracking. It is commonly assumed that much of this information is privacy sensitive and security breaches or data mismanagements

by administrators may lead to confidentiality breaches. Also users may not feel contented with their personal data being collected for security purposes. Thus, it would seem that security and privacy are conflicting requirements. This means that approaches to reconciling data security and privacy need to be looked into.

4. Data breach reporting and management strategies coupled with reviewing the ICT policy of businesses is another constituent that requires due consideration. It is important to also create awareness and advocacy and promote cyber security training and development. In many businesses, cyber security awareness takes the back seat. It is prudent to have more advocacy, and the need for stressing culture and behaviour change for dealing with cyber threats is critical.

5. Policy monitoring, evaluation and accountability are also vital for businesses to be able to evaluate the effectiveness of policies.

Marketing also predominantly takes precedence in cyber security matters for businesses and therefore advocacy and cyber security champions as well as creating cyber security awareness is pertinent. The following recommendations are made:

1. Businesses must create educational e-content which could be in the form of blogs, downloadable materials, webinars, video tutorials or businesses could prepare flyers and brochures to hand out to users. Businesses could also use local radio and talk back shows, TV and social media outlets to pursue the targeted audiences.

2. Advocacy could also relate to notifying the in-house staff as well as public about cyber security threats and the measures instituted by businesses.

3. Businesses could actively be engaged at their industry events or forums leading and participating in it to promote the business and share best practices in cyber security measures.

4. Encouraging training of the workforce to better comprehend cyber security threats and crimes is also essential. Marketing the training programmes is another important aspect.

5. Businesses also need to forge strategic partnerships with government agencies, ministries and policy-makers to design cyber security frameworks and policies as well as to identify threats to external networks. Targeting the audience would be an important part of marketing.

6. Businesses can also act as a close hub to furthering research and proposing solutions with think tank agencies on critical issues. Again, this information can be marketed via social media, blogs, presentations and workshops.

7. Business collaboration should be extended to NGO's, private sector and scientific organisations and donor agencies to build funding opportunities, enhance capacity building and promote shared practices.

8. Businesses as part of their marketing strategy also need to ascertain the feedback of their stakeholders and publicize successes and failures.

9. Businesses ought to document demonstrator projects or developments. For successful models, replication and scaling-up would be far easier. Such enterprises can be resource intensive as well.

Conclusion

In this contemporary era of technology, the pace at which the internet is being used as well as the predominant role of the internet globally has exposed businesses in developing countries to the cyber world where cyber criminals are accessing data and information rapidly. Cybercrime is no doubt an illegitimate act and a threat that warrants proper security to be embarked upon determinedly and meritoriously. There is a need to create more cognizance among the businesses and fundamentally the end users about internet and about the cyber space/internet of things, the varied forms of cybercrime and offcourse some precautionary measures as they use the internet. Security currently is becoming a protruding and foremost concern. In this paper, some security issues have been introduced. It is hoped that through proper policy and marketing drive, cyber threats would be affluently managed by businesses.

References

Adhikari, C. 2016. "Cybersecurity Challenges in Developing Countries". *ICT Frame*. Retrieved from: https://ictframe.com/cybersecurity-challenges-in-developing-countries/ (Accessed 30 September 2020)

Baur-Yazbeck, S. 2018. "Cyber Attacks Growing Problem in Developing Nations". ***IPS Inter Press Service News Agency.*** Retrieved from: http://www.ipsnews.net/2018/10/cyber-attacks-growing-problem-developing-nations/ (Accessed 24 September 2020)

Bharara, P. "Cyber Security: Protecting Our Cyber Citizens." *Advances in Cyber Security: Technology, Operations, and Experiences*, edited by D. Frank Hsu and Dorothy Marinucci, Fordham University Press, NEW YORK, 2013, pp. 226–234. Retrieved from: *JSTOR*, www.jstor.org/stable/j.ctt13x07xx.19. (Accessed 30 September 2020)

Catota, F.E, Morgan, G.M and Sicker, D.C. 2019. "Cybersecurity education in a developing nation: the Ecuadorian environment". *Journal of Cybersecurity*, 1-19. Retrieved from: doi: 10.1093/cybsec/tyz001. (Accessed 30 September 2020)

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

Chang, L., and Coppel, N. 2020. "Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar". *Computers & Security*. Retrieved from: 97. 101959. 10.1016/j.cose.2020.101959 (Accessed 29 September 2020)

Das, A., Saju, D., and Gupta, D. 2020. "A Study of Cyber Security and Its Challenges". *International Journal of Engineering Applied Sciences and Technology* 5:747-753. Retrieved from: 10.33564/IJEAST. 2020. V05i01.131 (Accessed 29 September 2020)

Dudley, T. 2020. "Users are an intelligence source: Are you leveraging them in your detection strategy?" *Cyber Security: A Peer-Reviewed Journal* 4(1): 40-47.

Ellefsen, I. 2014. The development of a cyber-security policy in developing regions and the impact on stakeholders. 1-10. Retrieved from: 10.1109/ISTAFRICA.2014.6880605 (Accessed 29 September 2020)

Finau, G., Samuwai, J. and Prasad A. 2013. "Cybercrime and its Implications to the Pacific. The Accountant". *The Journal of the Fiji Institute of Accountant.* Retrieved from: https://core.ac.uk/download/pdf/17345706.pdf (Accessed 01 October 2020)

Goodin, D. 2002. "Accounting firms fight cybercrime", *CNET News*, Retrieved from: http://news.cnet.com/Accounting-firms-fight-cybercrime/2100-1023_3-226713.html (Accessed 01 October 2020)

Harry, C. 2020. "The challenge of assessing strategic cyber security risk in organisations and critical infrastructure". *Cyber Security: A Peer-Reviewed Journal* 4 (1): 58-69.

Jbair, M. 2020. "Security monitoring strategies for your OT infrastructure". C*yber Security: A Peer-Reviewed Journal* 3 (3): 265-274.

Kayser, C. S., Ellen, M. M., and Cadigan, R. 2019-20. "Preventing cybercrime: A framework for understanding the role of human vulnerabilities". *Cyber Security: A Peer-Reviewed Journal*, 3 (2): 159-174.

Kortjan, N., and Solms, R. 2013. Cyber Security Education in Developing Countries: A South African Perspective. In: Jonas K., Rai I.A., Tchuente M. (eds) e-Infrastructure and e-Services for Developing Countries. AFRICOMM 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 119. Springer, Berlin, Heidelberg. Retrieved from: https://doi.org/10.1007/978-3-642-41178-6_30. (Accessed 01 October 2020)

Kumar, R. 2020. Cyber Security. Retrieved from:10.13140/RG.2.2.22162.20164. (Accessed 29 September 2020)

Lee, R. B. "Improving Cyber Security." *Advances in Cyber Security: Technology, Operations, and Experiences*, edited by D. Frank Hsu and Dorothy Marinucci, Fordham University Press, NEW YORK, 2013, pp. 37–59. Retrieved from: *JSTOR*, www.jstor.org/stable/j.ctt13x07xx.6. (Accessed 29 September 2020)

Lidong, W. and Randy, J. 2020. "Data analytics for network intrusion detection". *Journal of Cyber Security Technology*, 4 (2): 106-123, DOI: 10.1080/23742917.2019.1703525

MCIT, 2016, 'Samoa National Cybersecurity Strategy 2016-2021', Ministry of Communications and Information Technology, Government of Samoa, Retrieved from: https://mcit.gov.ws/wp-content/uploads/2019/04/Cybersecurity-Strategy_Final.pdf (Accessed 29 September 2020)

Muller, L.P. 2015. "*Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*", Norwegian Institute of International Affairs, Report no. 3, Retrieved from: https://cybilportal.org/wp-content/uploads/2020/06/NUPIReport03-15-Muller.pdf (Accessed 30 September 2020)

RSA, 2016, 'Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise', RSA EMC Corporation, United States of America, Retrieved from: https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf (Accessed 30 September 2020)

Tagert, A.C. 2010. 'Cybersecurity Challenges in Developing Nations', Unpublished Doctor of Philosophy Thesis, Department of Engineering and Public Policy, Carnegie Mellon University. Retrieved from: file:///C:/Users/e.groves/Downloads/Cybersecurity%20Challenges%20in%20Developing%20Nations%20(1).pdf (Accessed 30 September 2020)

Vazzana, J. 2019. "Securing Technology is No Longer a 'First World Problem". *New America Organization*. Retrieved from: https://www.newamerica.org/cybersecurity-initiative/humans-of-cybersecurity/blog/securing-technology-is-no-longer-a-first-world-problem/ (Accessed 30 September 2020)

Zareen, M., Monis, A., Muhammad, T., and Khalid, U. 2013. "Cyber security challenges and way forward for developing countries". 2013 2nd National Conference on Information Assurance (NCIA). 7-14. Retrieved from: 10.1109/NCIA.2013.6725318 (Accessed 30 September 2020)