American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-7, pp-257-260
www.ajer.org
Research Paper Open Access

Remarks on National Cyber Security for under Developed and Developing Countries: focused on Malawi

Kondwani Makanda[1], Thokozani Felix Vallent[2], Hyunsung Kim[2,3]
[1](Computer Science Department, Malawi University of Science and Technology, Malawi)
[2](Department of Mathematical Sciences, University of Malawi, Malawi)
[3](Department of Cyber Security, Kyungil University, Korea)
Corresponding Author: Hyunsung Kim

ABSTRACT: *Cyber security is an important issue and a major concern in today's connected world. In this paper, we present cyber security scenario for under developed and developing countries focusing mainly on Malawi. In this aspect, we look at a number of weaknesses that Malawi has in terms of cyber security. Much as there are so many positive things that are being done to improve cyber security in Malawi the weaknesses are so critical in that they can lead to major disruption to normal day to day lives of the citizen. In this paper we also found out that there is no major study done on the cyber security position of Malawi and this work will act as a starting point for more research on the cyber security of Malawi.*

Keywords: *National cyber security, cyber security strategy, Malawi cyber security*

Date of Submission: 18 -05-2017 Date of acceptance: 28-07-2017

I. INTRODUCTION

Cyber security is one of the most important concerns in our modern connected world that touches all aspects of our daily life [1]. No country is immune from the threats that come in the cyber space and computer security is fundamentally difficult to achieve and for developing countries like Malawi the threat is even bigger due to lack of the right infrastructure and lack of experts trained in handling cyber space security [2-4].

Cybercrime or threat was identified as a threat for underdeveloped countries like Malawi [1, 5]. Malawi is a landlocked country located in the south eastern part of Africa. It has a population of around 15,883,000 [6]. Internet users as a percentage of population stand at a low percentage of 5.40% [7]. Since Internet usage is still low even in comparison of the average among some African countries, it will mean that the number of users of Internet will have to increase [5]. Table 1 gives Internet penetration in Malawi as a comparison with other African countries. As it can be seen from the table, Internet usage is lower meaning the potential for growth is there.The increase in Internet users will come about due to the usage of mobile devices as a means of connecting to the Internet and also the many e-services that are being offered by the governments and private organizations [2-3].

Malawi currently has two cellular network operators with the third one yet to roll out [5]. With Internet service providers, Malawi has 46 registered Internet service providers although only 15 Internet service providers are operational [5]. The country has two fixed line telecommunication providers [5].

Table 1: ICT development in selected African countries **[**5].

Country	Fixed(Wired) Broadband Subscriptions	Percentage of Individuals using Internet	Mobile Cellular Subscription per 100 Inhabitants
Malawi	2,854	5.4	32.33
Botswana	21,590	15	160.64
Kenya	57,033	39	70.59
Swaziland	4,200	24.7	71.47
Nigeria	15,045	38	73.29

Zambia	10,850	15.4	71.50
Uganda	41,500	16.2	44.09
Tanzania	51,903	4.4	55.72
Mozambique	17,983	5.4	48.00

II. CYBER SECURITY STRATEGIES IN UNDER DEVELOPED AND DEVELOPING COUNTRIES

Similar to the rest of the world, Africa is also exposed to the risk of cyber-crimes/threats or attacks. This was identified as among the top 5 risks that African countries face [19]. In this section we are going to look at a number of African countries in relation to their cyber strategies.

The first country that we looked at is South Africa. South Africa faces almost the same challenges that other countries in the developing world faces. South Africa drafted the cyber security and cyber-crime bill in order to be able to regulate these fields [20]. South Africa also has the Protection of Personal Information Act (not enacted into law) which will help to ensure that all South African companies, organization and government agencies conduct in a responsible manner when processing, collecting, storing and sharing of individuals' private data [20]. This Act also holds the organizations accountable if any data is abused or compromised [20]. Although these bills were drafted the problem is that of enforcing these bills i.e. if a cyber-crime has been committed the government should be able to use this law to punish the perpetrators [20].

The second country that we are going to look at is Nigeria. [21]. Similar to South Africa, after seeing an increase in cyber-crime the Nigerian government introduced a bill in 2013 to help prevent and control cyber-crime [21]. This law faces similar challenges to the ones in South Africa i.e. weak implementation of the law and law enforcement agencies that are poorly equipped [21]. In [21], the also pointed out some of the information security challenges that are faced by developing countries which include the following, lack of lack of understanding as to what information security is by the general society, governments in developing countries lack direction in terms of implementation of information security policies and lack of interest in security education and training.

The next country that we are going to look at is Rwanda. Rwanda is one country whose policy makers believe that Information Communication Technology will help in creating jobs and economic prosperity and as such the government is distributing computers to all rural and poor areas [16]. Rwanda has the National Cyber Security Strategic Plan which aims to establish a National Cyber Security Agency (NSCA) which aims at: ensuring that planning, coordination and implementation of national cyber security policy/strategy, making sure that all legal and regulatory frameworks are in conformity with national and international cyber security standards, protecting national critical infrastructure and information systems and provide information security assessment of both private and public institutions [16, 22]. The country is also planning on establishing a national cyber-crime investigation center which will help in investigating cyber-crimes, help in retrieving and analyzing digital data [22].

If government data is stolen, there are a number of consequences that can happen. These include; databases containing citizen's data can be exposed, there can be unauthorized control of national infrastructure, cyber terrorism, disruption of healthcare if these systems are online and lastly other countries will not trust the country where data breach has occurred when it comes to sharing confidential information [20]. University's efforts to train people, any other directions from non-governmental bodies? Furthermore, whole sections should provide consistency by following the three or more perspectives.

III. MALAWI'S EFFORTS ON CYBER SECURITY

From our research, we did not manage to find a lot of literatures relating to cyber security for Malawi i.e. not much research on cyber security for Malawi has been written. A great summary of the cyber security position which includes some weaknesses and strengths are presented in [7].

One thing that was interesting for Malawi is that it has a number of national systems that can be affected by weak cyber security. In this part, we will look at some government systems that play an important role in the day to day running of government business. One of the systems that is used is the Integrated Financial Management System (IFMS) [8]. Currently, IFMS is being used at the central government level but there are plans to allow the system work nationally i.e. to allow payments to be made from a remote location. This system helps the government in budgetary, accounting and payment processes [8]. IFMS uses a password as a security protection to prevent unauthorized people from accessing the system. But the system is also on intranet as a security measure. Some of the users or managers who make approval to payments are prone to manipulation due to lack of knowledge in how to use computers and the importance of passwords.

The country is also embarking on a National Registration and Identification exercise where any citizen who is 18 year or above should be registered. This system will also need to be secured since some sensitive data will be stored [9].The other system used by government is the Malawi Traffic Information System (MalTIS). This is a system that is used for registering new vehicles, printing drivers' licenses and other functions relating to motor vehicles. This system is also linked to the Malawi Revenue Authority in order to check whether the owner of the vehicle has paid taxes when buying the vehicle. This is also another system that is crucial to the country and needs protection from cyber-crime [10, 23].The country has also introduced the Electronic Fiscal Devices (EFD). This is used by the Malawi Revenue Authority to improve on revenue collection by computerizing tax auditing processes, by reducing work for tax authority and increasing tax revenue [11].

All these systems and probably some that we did not mention in this paper will need to be secured to assist the country function properly. This paper is not a study of the systems mentioned above but the general study of how the country can secure these systems.

In this paper, we studied the cyber security position of Malawi, which looks at a number of issues affecting Malawi in the cyber security arena including laws that deal with cyber security, regulatory bodies in cyber space, training and education of cyber security experts, and strategies the country has for cyber security.

IV. PROPOSED CYBER SECURITY STRATEGIES FOR MALAWI

In this section, we look at some challenges and strengths that Malawi has in terms of cyber security. For legal measures, Malawi currently has cyber security law that aims at criminalizing cybercrime which was enacted by parliament in 2016 [12]. This is a move in the right direction but the problem is the lack of well trained and knowledgeable man power to be able to enforce the law i.e. there is lack of well-trained law enforcers to be able to carry out tasks like doing computer forensics to find evidence of malicious act and intrusion detection.

As noted in [7], much as there is a program that trains postgraduate students in cryptography and Information Theory, Coding and Cryptography. The undergraduate program currently being offered at the Malawi University of Science and Technology (MUST) is currently in first year. This means that the country has to wait three or more years before these trained cyber security graduates can be utilized [13-14]. All these programs will help Malawi educate cyber security personnel which will be crucial in protecting the cyber space of the country. Currently MUST has a number of courses that are being taught to undergraduate computer security students which include but not limited to the following, Hardware Engineering, Operating Systems, Data Structures & Algorithms, Databases Systems, Database Administration, Computer Networks, Cryptology, Computer Security, Artificial Intelligence, Ethical Hacking, System Audit, Software Reverse Engineering, Data Compression, Mobile & Wireless Network Security, Digital Forensics and Network Security.

Based on our research we also find out that Malawi still does not have Computer Security Incident Response Team (CSIRT) [15]. The CSIRT if created will act as a central point where all cyber security issues dealing with the country will be coordinated. This can include issues like having a call center where citizens can call to get help in relation to cyber security issues. It can also help companies or organizations that don't have cyber security expertise when they have experienced any cyber security breach and they need assistance.

Due to lack of cyber security experts in Malawi, policy makers in these developing countries lack better guidance in how to secure their cyberspace [16].

In terms of regulation and compliance, Malawi does not have any regulation and compliance body regarding cyber security [7, 15]. At the moment Malawi does not have any internationally certified government and public sector agencies in terms of cyber security [15] which according to our research is still the same. This still remains the same as the paper was being prepared. For cyber security policies, Malawi has the Malawi Information Communication Technology Policy as a guiding policy [17]. Malawi has the Malawi Communication Regulatory Authority (MACRA) as an agency mandated to implement regulatory functions over telecommunications, broadcasting, postal, Internet and managing of the radio frequency spectrum of the country. It was established by an act of parliament which was enacted in 1998 [5, 18].

Malawi has also another weakness in the mobile phone area as anyone can easily buy a Subscriber Identification Module (SIM) card on the street and use it to connect to Internet without registration with a government or even the mobile communication provider. This is a weakness since the unregistered SIM card can be bought and used by people with malicious intent who can end up causing material and financial damage to individuals and organization. These people cannot be traced and tracked since the SIM they were using we not registered.During our research we find out that once the data in the Integrated Financial Management System is saved it is not encrypted. This is a weakness since once one has the database he or she can easily manipulate the data thereby causing financial damage to the system.

Since cyber security in international in nature, Malawi takes part in a number of cyber security workshops including the International Telecommunications Union IMPACT (ITU-IMPACT) initiative which provides access to cyber security services which are important to Malawi [7]. Malawi also participates in regional cyber security workshops like the Common Market for East and Southern African (COMESA) Cyber Security and Public Key Infrastructure Meeting [7].

V. CONCLUSIONS AND REMARKS

Much as Malawi has a number of challenges in regard to cyber security, it has a better chance of implementing good policies, strategies and measures due to the low number of devices, systems and infrastructure devices that are online. Malawi should aim to train more cyber security experts if the country is to stay ahead of hackers and other people who may have malicious intent towards the country. Malawi should also aim to create bodies that will be fully mandated to carry out functions regarding cyber security monitoring, preparedness and protection of the country.

ACKNOWLEDGEMENT

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

REFERENCES

[1] *Cyber Security Guide For Developing Countries*(International Telecommunication Union, Edition 2007).

[2] J. Coertze, R.v. Solms, A Model for Information Security Governance in Developing Countries, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 119*, 2012, 279-288.

[3] H. Hussain, *Dialing Down Risks: Mobile Privacy and Information Security in Global Development Projects*(New America Foundation, August 2013).

[4] M. Gasser, *Building a Secure Computer System*(Van Nostrand Reinhold, 1988).

[5] *Strategic Plan 2015-2020* (Malawi Communication Regulatory Authority,http://www.macra.org.mw/wp-content/uploads/2014/09/MACRA-Strategic-Plan-2015-2020.pdf).

[6] *United Nations Statistics Division*, (December 2012, http://unstats.un.org/unsd/demographic/products/socind/default.htm).

[7] *International Telecommunications Union Statistics* (2013, http://www.itu.int/ITU-D/ict/statistics/).

[8] J. Diamond, P. Khemani, *Introducing Financial Management Information Systems in Developing Countries*(International Monetary Fund, October 2005).

[9] Malawi Government, http://www.malawi.gov.mw/index.php?option=com_content&view=article&id=31&Itemid=115, Accessed 17th May, 2017.

[10] Directorate of Road Traffic & Safety Services, http://www.drtss.gov.mw/mvr.php, Accessed 17th May, 2017.

[11] Electronic Fiscal Devices, http://www.mra.mw/business/electronic-fiscal-devices-efds, Accessed 24th April, 2017.

[12] Electronic Transaction and Cybersecurity Act, 2016. http://www.malawilii.org.mw/legislation/act/2016/33, Accessed 24thApril, 2017.

[13] MUST Bachelor Program on Computer Systems and Security, http://www.must.ac.mw/programme/bachelor-of-science-in-computer-systems-and-security, Accessed 25thApril, 2017.

[14] Mzuzu University, http://www.mzuni.ac.mw, Accessed 25thApril, 2017.

[15] ITU, *Cyber Wellness Profile Malawi*(ITU, 2014).

[16] A.C. Tagert, *Cybersecurity Challenges in Developing Nations*,Doctoral Dissertation, Carnegie Mellon University, Pittsburgh, PA, 2010.

[17] Malawi Government, *National ICT Policy* (Malawi Government, 2013).

[18] Malawi Communications Regulatory Authority, http://www.macra.org.mw, Accessed 27th April, 2017.

[19] South Africa Government, *Africa Risk in Review 2015*(PricewaterhouseCoopers South Africa, 2015).

[20] South Africa Government,*South Africa Risks 2016* (Institute of Risk Management South Africa Risk Report, 2nd Edition, 2015).

[21] I.J. Ikenwe, O.M. Igbinovia, A.A. Elogie, Information Security in The Digital Age: The Case Of Developing Countries,*Chinese Librarianship: an International Electronic Journal, 42*, 2016, 16-24.

[22] Republic of Rwanda, *National Cyber Security Strategy*(Republic of Rwanda, Kigali, 2015).

[23] Directorate of Road Traffic and Safety Services, http://196.30.218.12:8080/WEBSITE/home.jsf, Accessed 27th April, 2017.

Kondwani Makanda. "Remarks on National Cyber Security for under Developed and Developing Countries: focused on Malawi." American Journal of Engineering Research (AJER) 6.7 (2017): 257-260.