World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:3, 2019

Cybersecurity Protection Structures: The Case of Lesotho

N. N. Mosola, K. F. Moeketsi, R. Sehobai, N. Pule

***Abstract*—**The Internet brings increasing use of Information and Communications Technology (ICT) services and facilities. Consequently, new computing paradigms emerge to provide services over the Internet. Although there are several benefits stemming from these services, they pose several risks inherited from the Internet. For example, cybercrime, identity theft, malware etc. To thwart these risks, this paper proposes a holistic approach. This approach involves multidisciplinary interactions. The paper proposes a top-down and bottom-up approach to deal with cyber security concerns in developing countries. These concerns range from regulatory and legislative areas, cyber awareness, research and development, technical dimensions etc. The main focus areas are highlighted and a cybersecurity model solution is proposed. The paper concludes by combining all relevant solutions into a proposed cybersecurity model to assist developing countries in enhancing a cyber-safe environment to instill and promote a culture of cybersecurity.

***Keywords*—**Cybercrime, cybersecurity, computer emergency response team, computer security incident response team.

I. Introduction

THE world is very much connected than ever before. The Internet is the fastest growing infrastructure which services almost all aspects of our lives [1]. For example, people shop online, learn online, get health-related information online etc. Developing countries are increasingly investing in the use of Internet-based services. Various countries are investing in telecommunications and the Internet as they are rapidly adopting electronic services. Through the use of the Internet, the cyberspace is growing at an unprecedented speed. Although there are numerous benefits that the Internet brings, there are equally more challenges that come with it. The challenges include unethical and illicit activities such as cyber stalking, illegal trades and cyber espionage etc. These challenges can be reduced by being cautious and commissioning cybersecurity awareness among Internet users.

Cybersecurity is a field specializing in protection of Internet-based systems, companies, and individuals from cyberattacks [2]. Cyberattacks include unauthorized access, malware attack, botnets, phishing etc. [2]. The protection of personally identifiable information, which is any piece of information that can be used to distinguish or uniquely trace an individual's identity, is at the helm of cybersecurity.

The aim of this paper is to take a first step towards a better understanding of the reasons behind cybersecurity awareness. It proves the importance of cybersecurity awareness and how developing countries can effectively implement cybersecurity measures. Lesotho is a small, completely land-locked country with a population of 2 million [4]. Lesotho has a low penetration of ICTs, albeit it is growing in terms of mobile technologies. Currently there is no legal framework regarding cybersecurity in Lesotho [5]. The same applies for many other developing countries, especially in the African context. There is little to no cyber awareness campaign in Lesotho. Thus, citizens are not aware of the cyber risks they are exposed to. Therefore, the need for cybersecurity awareness cannot be disputed. Cyber awareness remains one of the main defense mechanisms in providing businesses, organizations and individuals with relevant information on how to protect information, electronic assets and staying safe online [6].

Although cybersecurity is a global agenda, this paper focuses on cybersecurity issues having both direct and indirect impact on people and systems connected to the Internet, with a focus on developing countries. It investigates a number of current cybersecurity problems faced by developing countries and how they can come up with a working cybersecurity awareness model. The paper is structured as follows; Section II reviews existing literature in cybersecurity. Section III covers cybersecurity issues in Lesotho. Section IV proposes cybersecurity structures. Section V discusses a holistic approach towards building cybersecurity structures. Section VI introduces the proposed cybersecurity model. Section VII concludes the paper.

II. Literature Review

Contrary to developed countries, developing countries face several challenges to develop and implement cyber safety initiatives. This is a result of developing countries being characterized by limited resources, capacity, expertise and understanding of cyber security [7], [8]. However, developing countries are adopting use of new and sophisticated technologies at a high speed. There is a high technological growth in developing countries as many are utilizing Internet-based services. Despite the increasing growth, many of these countries do not have the capacity to implement cyber protective structures. These structures are used to effectively manage new technological trends and the security risks they bring.

To mitigate some of the cybersecurity threats in developing

N. N. Mosola is a lecturer in computer science at the National University of Lesotho (corresponding author, phone: +26658606670; e-mail: nn.mosola@ nul.ls, Cc: nmosolan@gmail.com).

K. F. Moeketsi is a Lecturer in computer science at the National University of Lesotho (e-mail: fk.moeketsi@nul.ls).

R.Sehobai is a Bachelor of Engineering in Electronics student at the National University of Lesotho (e-mail: nattysehobai347@gmail.com).

N. Pule is with the Lesotho Communications Authority, Universal Services Fund, Lesotho (e-mail: npule@lca.org.ls).

countries, it is recommended that implementation of cybersecurity awareness and training programs is a top priority [9]. The government has a huge role to play, to foster large-scale awareness about cybersecurity and incorporate it into the core curriculum of academic institutions, as soon as students begin using computing and electronic devices [10]. Through well-coordinated cybersecurity awareness programs, cybercrime can be mitigated, as most security breaches are often due to lack of knowledge rather than a deficiency in the systems being used [11]. Furthermore, the issue of regulation and legislative frameworks has to be considered by government. Governments need to put in place robust legislative measures against cybercrimes and ensure that cyber policies keep pace with rapidly evolving technology [12]. To protect the nation from cyberattacks, cybersecurity regulations have to be in place. Such regulations ensure that organizations protect their digital resources, data, systems, networks etc., following globally accepted standards [13].

III. Situational Analysis on Cybersecurity Problems in Lesotho

Similar to any country, Lesotho is not an exception when it comes to cyber-related issues. Increased digitization in Lesotho has led to the increase in the usage of mobiles devices, web-based systems etc. The government is moving towards providing services through electronic means, a move known as e-Governance. Thus, Lesotho is increasing the attack surface. Cyber criminals can target anyone accessing a government service online. Therefore, as part of the electronic governance structure, cybersecurity measures should be a great concern. Some of the cybersecurity issues in Lesotho are discussed below:

A. Lack of Focused Cybersecurity Research

There is little to no focused research within the cybersecurity space. At national level, there is no research being conducted to protect Lesotho against known and future cyber-attacks. This makes Lesotho to be more vulnerable to most cyberattacks as there is no knowledge stemming from research findings on cybersecurity despite increasing use of Internet-based services and high mobile phone penetration statistics. Fig. 1 depicts the mobile phone usage in different age groups in Lesotho. Fig. 1 shows the increasing use of mobile phones in Lesotho. This in turn gives insight that perhaps Internet use in Lesotho is exponentially increasing most mobile phones provide Internet connectivity.

B. Lack of Cybersecurity Awareness

Many people, young and old, have fallen victim to various cybercrimes due to their lack of awareness [15]. Most of Lesotho's citizens are not aware of the inherent risks that come with accessing services electronically. Lack of awareness campaigns in the country does not ensure a culture of cybersecurity. There is no leading organization, public or private, taking the responsibility of making people aware of the cybersecurity issues the country faces. Awareness plays a big role in cyber defense as most of the time, cyberattacks are not a result of a deficiency in the systems used but lack of knowledge by the users. Thus, education about risks and dangers that come with cyberspace is vital in today's world of increasing use of cyberspace [16]. Fig. 2 shows the increasing number of Internet users in Lesotho. More people are accessing services online as most of the government services are now provisioned online, in the quest to have electronic governance (e-Governance) solutions [17].

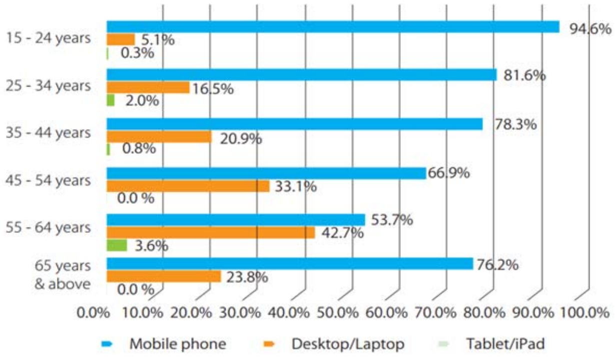
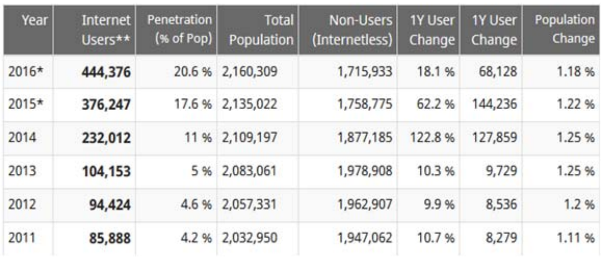


Fig. 1 Mobile phone penetration in Lesotho [14]



Year	Internet Users**	Penetration (% of Pop)	Total Population	Non-Users (Internetless)	1Y User Change	1Y User Change	Population Change
2016*	**444,376**	20.6 %	2,160,309	1,715,933	18.1 %	68,128	1.18 %
2015*	**376,247**	17.6 %	2,135,022	1,758,775	62.2 %	144,236	1.22 %
2014	**232,012**	11 %	2,109,197	1,877,185	122.8 %	127,859	1.25 %
2013	**104,153**	5 %	2,083,061	1,978,908	10.3 %	9,729	1.25 %
2012	**94,424**	4.6 %	2,057,331	1,962,907	9.9 %	8,536	1.2 %
2011	**85,888**	4.2 %	2,032,950	1,947,062	10.7 %	8,279	1.11 %

Fig. 2 Internet users in Lesotho [17]

C. Lack of Cybersecurity Technical Skills

Skills shortages are not purely experienced in developing countries alone, as developed countries still have such shortages. However, it is in the developing world where there is massive impact, for example, in Lesotho. The country is heavily hit by the lack of technical skills in the cybersecurity arena. ICT and related areas are some of the hardest areas hit by skills shortages. Capacity building in terms of professional skills in cybersecurity is very low. There is currently no local institution of higher learning offering any curriculum or training in cybersecurity.

In the absence of required technical skills, Lesotho will not be able to implement any national cybersecurity strategy or have any form of a cybersecurity defense structure. To address this, Lesotho may out-source such skills as it is unable to groom its own personnel due to financial or other impediments. To some extent, local trainings are hindered by low levels of basic education or low turn-over of graduates from ICT-related fields. This seems to be a problem in many developing countries as they face several challenges to develop and implement cybersecurity initiatives due to being characterized by limited knowledge, lack of expertise and no understanding of cybersecurity [7]. The development and effective management of national cybersecurity structures depends on how well countries acquire and retain technical skills. Lack of technical cybersecurity skills in Lesotho implies inadequate skills and insufficient technology needed to thwart cyberattacks. For example, the security sectors, made up of the national police, the army, security services etc., is not well equipped with highly qualified personnel to curb cyberattacks and defend the country against advanced persistent attacks (APTs) at the national level.

D.Lack of Cybersecurity Legislation and Regulatory Framework

A major hindrance towards achieving a culture of cybersecurity is the lack of legislative and regulatory frameworks. This refers to both cybersecurity policies and legislation. Due to the Internet maturing in developing countries, there is an increased attack surface around respective the country's critical infrastructure (CI). Developing countries have begun to establish various cybersecurity policies, programs, and initiatives (PPIs). Thus, there is a need to implement legislative measures to regulate the cyber space. For example, in Lesotho, as more people get e-Services, the government needs to review and implement legislation to regulate Internet-based services. Though the government of Lesotho has drafted the Computer and Cyber Crime Bill, Electronic Commerce and Transactions Bill etc., which seek to provide a legal framework to criminalize computer and network-related crimes, to date, Lesotho lacks adopted laws to regulate and specify cybercrimes [18]. Thus, Lesotho as a developing country needs proper and relevant laws, policies and practices if it is to successfully fight cybercrimes. The absence of legislative regulations in place to prosecute online crimes provides a safe haven for cyber criminals. However, even in the presence of any legislative and regulatory framework, the absence of a cybersecurity strategy in Lesotho renders the country vulnerable to sophisticated cyberattacks. Therefore, countries like Lesotho need to develop cybersecurity strategies, detailing how they aim to defend themselves against any form of cyber attack.

IV. Proposed Cybersecurity Structures

This section proposes the inception and adoption of national cybersecurity structures. National cybersecurity structures fall into several classes/categories. These categories are constructed in different ways. Each category serves the environment in which the structure is deployed. National cybersecurity structures can be decomposed into different components. However, the component this paper proposes is a Computer Security Incident Response Team (CSIRT), which is sometimes referred to as a Computer Emergency Response Team (CERT). The main role of a CSIRT is to provide security incident response capabilities. Among its roles, a CSIRT is tasked with providing a national cybersecurity culture and dissemination of any security-related information and management [25], [26]. To help in broadcasting information related to cybersecurity, a CSIRT must also form part of a research team in a cybersecurity research centre. To expand the body of knowledge in terms of cybersecurity and increase national research output; a center for cybersecurity research is proposed. The aim of the center is to offer research and development at the national level in terms of cybersecurity and related areas. Moreover, the center will ensure a culture of cybersecurity in Lesotho [19]. The center is the central hub and contact point where all aspects related to Critical Information Infrastructure Protection (CIIP) and cybersecurity issues are coordinated. The center is the sole provider of the expertise in the realm of cybersecurity. Personnel in the center are equipped with vast amounts of technical cybersecurity and academic background. The center provides a platform where knowledge and ideas can be brainstormed and shared among participating entities to keep the nation up-to-date on any discoveries on how to counter cyber threats brought by the use of Internet-based services. The center may have the following initiatives: cybersecurity awareness, assist in cybersecurity policy development, information sharing and cyber intelligence, national cybersecurity research and publication of reports etc.

The aspect of cybersecurity awareness can be handled using a bottom-up approach, using a structure known as Community-Oriented Security, Awareness and Warning (C-SAW). C-SAWs are a possible solution to addressing awareness problems as they boost cybersecurity awareness and willingness to develop a cybersecurity culture within communities, especially those with little or no knowledge of ICT skills. This solution focuses mainly on individuals with little or no cybersecurity knowledge or background. An awareness and training program is crucial in that, it is the simplest way of circulating information to end-users. Development of specialized cybersecurity courses in local universities and colleges as well as in primary and secondary school curricula qualifies as one of the awareness approaches [20]. Awareness presentations are intended to allow individuals to recognize cybersecurity concerns and respond accordingly [3]. Thus, people need not only be aware of cyber risks but also to acquire adequate knowledge to use the cyberspace accordingly [21]. Hence, it is important that users are assisted to connect to the Internet by complying with specific regulations and awareness principles in an attempt to decrease cybercrime. This is one of the functions a CSIRT can perform. Fig. 3 depicts a top-down approach towards creating a CSIRT. Fig. 3 depicts various cybersecurity structures which can be created to deal with cyber incidents. The model is generic, and thus, it can be deployed in various developing countries such as Lesotho. Entities such as the national cybersecurity council (NCSC) are responsible for reporting all matters related to cybersecurity from the various CSIRTs to government.

Another great aspect of cybersecurity structures is enforced by government through regulators. In the country in this study, the Lesotho Communications Authority (LCA) is the only ICT regulator. The task of the LCA is wide and varied. For example, the government of Lesotho should focus mainly on using regulating bodies such as the LCA to assist cyber users in their responsibilities regarding cyber use. Internet Service Providers (ISPs) and other regulating bodies could help cyber users to deal with the responsibilities they are not capable of implementing without some assistance. ISPs can have a much wider impact on the overall state because of their advantageous position in the network (that is, acting as the gateway to the Internet) [22]. Thus, their involvement will improve cybersecurity awareness if government works hand-in-hand with the LCA and other regulators such as ISPs. Additionally, as there are currently no legal policies regarding cybersecurity in Lesotho, it would be better to begin establishing and enforcing them. An adequate legislative framework that can pass decisions for building a secure cyberspace is vital. A solid cybersecurity regulatory framework can serve as a backbone of cybersecurity [23]. To have a fully-fledged cybersecurity protection structure, a holistic approach towards treating some of the ailments in cybersecurity is proposed. The next section discusses a holistic approach towards building cybersecurity protection structures.

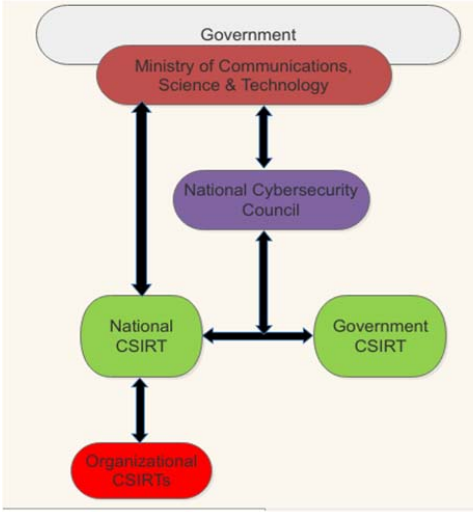

Government
Ministry of Communications, Science & Technology
National Cybersecurity Council
National CSIRT
Government CSIRT
Organizational CSIRTs

Fig. 3 National CSIRT and coordination

V. Holistic Approach to Cybersecurity Structures

Each of the investigated cybersecurity structures in the previous sections contributes a unique cyber focus aspect in the attempt to address cybercrimes in Lesotho. The different cybersecurity focus aspects include: Shared body of knowledge, awareness and cybersecurity capacity building, cybersecurity defense and intelligence, legislative and regulatory framework etc. These focus aspects when grouped together form the basis for the proposed cybersecurity model to assist in the prevention of cybercrime in Lesotho. Fig. 4 depicts a holistic approach in developing cybersecurity structures, CSIRTs and C-SAWs.

The next section discusses a proposed model to follow to manage cybersecurity at a national level.

VI. Proposed Cybersecurity Model

The cyber-security model proposed in this section comprises three pillars vital for cyber-security which help in order to prevent and respond to cyber threats. These pillars are a combination of all the focal points derived from different approaches examined in the paper. These focal points are some of the solutions that other countries are using. The three pillars identified are: Role players, action plans and cyber-security body of knowledge (BOK).

The first pillar is the role players. These include all people and stakeholders with a role and responsibility to ensure cyber safety for cyber users. The role players include government, educational institutions, the public sector, national security agencies and the judiciary. Cybersecurity is a multi-faceted paradigm which requires concerted efforts from different role players, each having a specified role to execute.

The government must enforce cybersecurity policies, laws, strategies and frameworks to ensure a more secure cyberspace that supports national security priorities and the pro-active measures of combating cybercrime and prosecuting cybercriminals.

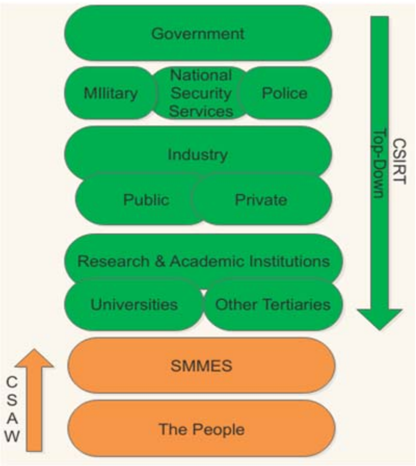


Fig. 4 A holistic approach to building cybersecurity structures

Educational or academic institutions also have a mammoth task to execute to ensure that enough capacity and skills are acquired. A well designed cybersecurity curriculum and coordinated professional training in cybersecurity should be the mandate of such institutions. Workshops and trainings on building and maintaining a cybersecurity culture and workforce must be provided as a mechanism to providing secure use of the cyberspace.

To help the government in building cybersecurity strategies, institutions of higher learning have to play a big role of skills transfer and capacity building in the country [24]. This will increase the number of cybersecurity professionals and help in the inception of cybersecurity protection structures such as computer security incident response teams (CSIRTs), which countries need to defend their national critical information infrastructure (CII) against cybercriminals.

The private sector has the infrastructure required for cybersecurity. Therefore, the role of the private sector in supporting protection structures can be carried out easily, to support government initiatives. Indeed, there is no silver bullet in security. Public-private partnerships (PPPs) are necessary in order to have a cyber-safe environment.

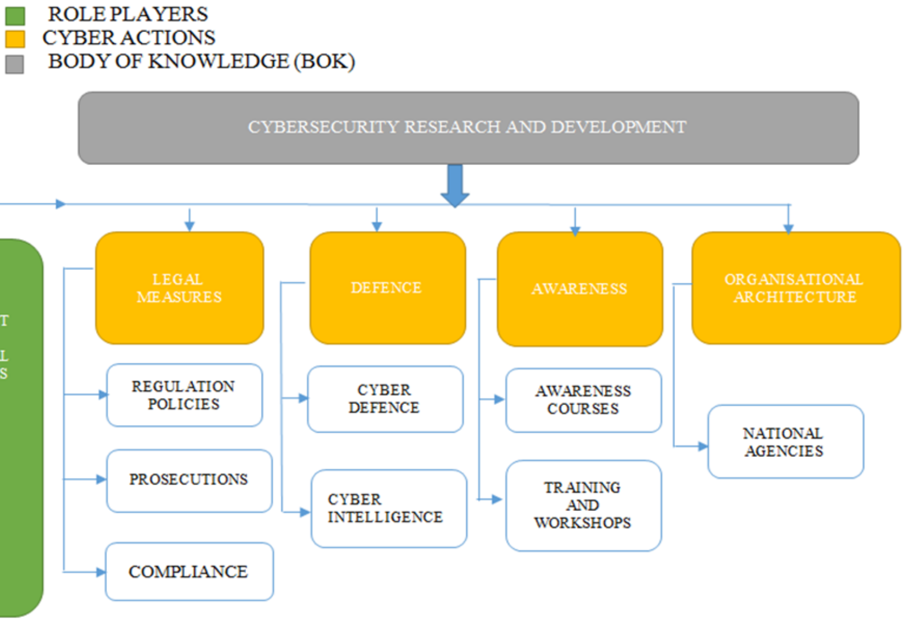


Fig. 5 Proposed cybersecurity model for Lesotho and developing countries

National security agencies in a country must be equipped with the capacity to handle security challenges at the national level [25]. In Lesotho, the national security services (NSS) is one of the law enforcement agencies (LEA) mandated with protecting national assets. However, the NSS is not yet capacitated to the level of handing advanced persistent attacks and protecting the country's critical information infrastructure. The NSS should also have mechanisms of cyber intelligence in order to detect, deter and respond to cybersecurity incidents. In collaboration with the local police services (Lesotho Mounted Police Services – LMPS) and the army (Lesotho Defense Force – LDF), enough cybersecurity intelligence technical workforce can be created as part of a CSIRT.

The judiciary is another big role player. The judiciary must have knowledge on cybersecurity in order to prosecute cybercriminals.

Currently, Lesotho does not accept digital evidence in the courts of law. Thus, the government needs to move fast in the process of passing the draft computer crime and cybersecurity bills to be adopted as law in the country so as to criminalize cybercrime.

The research conducted herein shows that if all the pillars depicted in Fig. 5 are implemented successfully, a secure cyberspace and a culture of cybersecurity will be achieved. All the strategies mentioned need to be implemented in a holistic manner, as Fig. 4 suggests, for a resilient cyberspace and an enhanced national cybersecurity. Moreover, countries need to consider conducting research in cybersecurity as all strategies ought to be well researched. All role players have to commit towards increasing national research output. The importance of this element cannot be overlooked as technology is rapidly evolving. Thus, countries need to be ahead of the technology curve through research.

VII. Conclusion

Technology is being adopted by many citizens in developing countries. New technologies emerge and governments provide services online. As new paradigms emerge, new cybersecurity risks surface. Therefore, the increasing need for cybersecurity protection structures proposed in this paper is undisputable. The research conducted through this paper concludes that cybersecurity must be included in all areas of society as it is a multi-disciplinary area. Thus, this paper concludes that developing countries such as Lesotho will benefit from the development and adoption of cybersecurity protection structures as discussed in previous sections. This research also proposed an encompassing model for Lesotho and other developing countries to assist in addressing the rapid increase in cybercrime. Therefore, it is important to have different cyber prevention aspects and integrate them into a multi-dimensional implementation plan, in the quest to raise and promote cyber safety, cyber awareness, capacity building, research and development and assist developing countries in promoting a cybersecurity culture. The importance of this research cannot be overemphasized as cybersecurity is a burning issue in most developing parts of the world.

References

[1] O. Szumski, "*Cybersecurity best practices among Polish students*," *Procedia Comput. Sci.*, vol. 126, pp. 1271–1280, Jan. 2018W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2] "Difference Between Cyber Security and Computer Science." (Online). Available: https://www.ecpi.edu/blog/difference-between-cybersecurity-and-computer-science. (Accessed: 02-Feb-2019). B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[3] M. Bada and A. Sasse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," 2014.

[4] "Lesotho Bureau of Statistics." (Online). Available:

http://www.bos.gov.ls/. (Accessed: 15-Feb-2019).

[5] "Lesotho cyber-wellness profile." (Online). Available: https://www.lca.org.ls/CYBERWELLNESS PROFILE.pdf. (Accessed: 15-Feb-2019).

[6] R. Chandarman and B. Van Niekerk, "Students' cybersecurity awareness at a private tertiary educational institution," Afr. J. Inf. Commun., vol. 2017, no. 20, pp. 133–155, 2017.

[7] M. J. Z. de Barros and H. Lazarek, "A Cyber Safety Model for Schools in Mozambique," 2018.

[8] E. Sutherland, "Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3201310, Jun. 2018.

[9] "Investigating the efficacy of cybersecurity awareness training programs -ProQuest." (Online). Available: https://search.proquest.com/openview/96d92f6796e45364234f187e94b401d8/1?pq-origsite=gscholar&cbl=18750&diss=y. (Accessed: 15-Feb-2019).

[10] S. Kouttis, "Improving security knowledge, skills and safety," Comput. Fraud Secur., vol. 2016, no. 4, pp. 12–14, Apr. 2016.

[11] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," Comput. Hum. Behav., vol. 48, pp. 51–61, Jul. 2015.

[12] C. McIntosh, "Cybersecurity: who will provide protection?," Comput. Fraud Secur., vol. 2015, no. 12, pp. 19–20, Dec. 2015.

[13] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," Future Gener. Comput. Syst., Oct. 2018.

[14] "ICT Research," (Online). Available: www.lca.org.ls/publications. (Accessed: 21-Feb-2019).

[15] "Lack of cyber security awareness cause of persistent online scams – Minister." (Online). Available: http://www.ghanaweb.com/GhanaHomePage/NewsArchive/Lack-of-cybersecurity-awareness-cause-of-persistent-online-scams-Minister-689408?channel=D1. (Accessed: 24-Feb-2019).

[16] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," J. Organ. Comput. Electron. Commer., vol. 28, no. 3, pp. 269–282, 2018.

[17] "Lesotho Internet Users." (Online). Available: http://www.internetlivestats.com/internet-users/lesotho/. (Accessed: 24-Feb-2019).

[18] "Cyber security under spotlight," *Lesotho Times*, 07-Apr-2017. (Online). Available: lestimes.com/cybersecurity-under-spotlight/. (Accessed: 24-Feb-2019).

[19] J. C. Jansen van Vuuren, M. Grobler, L. Leenen, and J. Phahlamohlaka, "Proposed Model for a Cybersecurity Centre of Innovation for South Africa," 2014, pp. 293–306.

[20] "Africa CyberSecurity Report 2016." (Online). Available: www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf. (Accessed: 24-Feb-2019).

[21] B. Pretorius and B. van Niekerk, "Cybersecurity for ICS/SCADA: A South African Perspective," Int. J. Cyber Warf. Terror. IJCWT, vol. 6, no. 3, pp. 1–16, Jul. 2016.

[22] "What Role Should ISPs Play in Cybersecurity?," Dark Reading. (Online). Available: https://www.darkreading.com/endpoint/what-role-should-isps-play-in-cybersecurity/a/d-id/1328716. (Accessed: 24-Feb-2019).

[23] L. P. Muller, "*Cyber Security Capacity Building in Developing Countries*," p. 4, 2015.

[24] R. Sabillon, V. Cavaller, and J. Cano, "National Cyber Security Strategies: Global Trends in Cyberspace," vol. 5, no. 5, p. 15, 2016.

[25] M. D. Mahlobo, "*National Cybersecurity Policy Framework*," p. 30, 2015.

[26] G. Killcrece. "*Steps for Creating National CSIRTs*". Coordination Center, 2018 (Online). (Available: www.cert.org/archives/pdf/NationalCSIRTs.pdf). (Accessed: 22-Feb-2019).