International Journal of Sciences:
Basic and Applied Research
(IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

Cybersecurity Challenges Facing Sub Saharan Africa: Botswana Context

Dr. Thulaganyo A. Rabogadi*

DBA (USA), MBA (UK), BEng (UK), CBRM, P .O. Box 4116, Gaborone, Botswana

Email: trabogadi@gmail.com

Abstract

The Global Cybersecurity Index (GCI) of Botswana dropped from position 23 in 2014 to position 69 in 2017 with GCI scores of .176 and .430 respectively. The mediocre GCI performance of Botswana resulted in modest GCI scores across all GCI competitive measures namely: legal, technical, and organizational structure, capacity building, and international cooperation. Generally, cybercrime exploits critical infrastructure systems, thereby placing the nation’s security, economy, public safety and health at risk. The absence of a national cybersecurity policy framework that describes the current security posture, identifies and prioritizes opportunities for improvement, and communicates to stakeholders about cybersecurity risk, may exacerbate the delay in the execution of Botswana National Cybersecurity Strategy, which has been under development for more than 3 years. The purpose of this qualitative multiple case study was to explore policy frameworks developing countries use to guide the development of cybersecurity policy and strategies organizations use to safeguard and combat cybercrime. Fifteen senior managers from the University of Botswana, Ministry of Transport and Communication, Botswana Police Service, Attorney General’s Chambers, and representatives from the private sector participated in a focus group interview during the 3rd International Conference on Internet, Cybercrime, and Information Systems hosted by University of Botswana on 1st to 2nd November 2018. Themes that emerged included awareness and training, fast tracking the approval of the National Cybersecurity policy, protecting government ICT infrastructure from incidents of cybercrime, building national computer emergency response teams and national security operations centers with appropriate governance structure, and the development of National Cybersecurity Policy to improve Botswana’s security posture and GCI performance.

Keywords: Cybercrime; Global Cybersecurity Index; Cybersecurity; Critical information infrastructure; Cyberattacks.

----

* Corresponding author.

1. Introduction

Botswana is among the fastest growing economies in the Sub Saharan Africa that strive to transform and strengthen socioeconomic and technological developments through the development of information and communication technology (ICT). Effective application of the Global Cybersecurity Framework, however, remains elusive. Despite high levels of exposure to cybercrime; advancements in technology, hyper-connected ICT infrastructure, and exponential growth in broadband and cellular mobile technologies exponentially emerge as strong drivers of economic growth in Botswana. Gartner predicted 60% of digital businesses would suffer major service failures due to the inability of security teams to manage digital risk [33].

Consequently, sensitive information still transverse open public and private computer networks and are delivered onto unsecure desktops and mobile devices, resulting in the abuse and compromise of data confidentiality, integrity, and availability. Cybersecurity in the cyberspace environment strives to ensure the attainment of security properties of the organization’s critical information assets [13; 28].

Efforts made to eliminate cybercrime, however, continue to increase especially in the domain of Internet diffusion [28:211]. The limited understanding and awareness of cybercrime, despite its devastating consequences, resulted in a lack of planning and development of policy framework to safeguard critical information assets [6]. The absence of a national cybersecurity policy framework that “describes the current security posture, identifies and prioritizes opportunities for improvement, and communicates to stakeholders about cybersecurity risk” [29:2], may exacerbate the delay in the execution of Botswana National Cybersecurity Strategy [19].

2. Problem Statement

Despite its overwhelming consequences on socioeconomic development, the limited understanding and awareness of cybercrime and cybersecurity substantially exacerbate lack of planning and development of an appropriate policy framework to safeguard critical information assets [7].

According to [26], the cost of cybercrime to the world economy is estimated at US$500 billion, more than the gross domestic product (GDP) of South Africa (US$350.6 billion) and a little less than the GDP of Nigeria (US$521.8 billion). Cybercrime is estimated to cost businesses US$2 trillion by 2019 [26]. For example, “in 2015, the British insurance company Lloyd’s estimated that cyberattacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business” [26: para 3]. Thus, the manifestation of cybercrime and its devastating capacity for causing harm to critical information assets caught most governments in the Sub Saharan Africa off guard [1].

The Global Cybersecurity Index (GCI) of Botswana dropped from position 23 in 2014 to position 69 in 2017 with GCI scores of .176 and .430 respectively [12;13]. The general business problem is the absence of a cybersecurity policy framework that defines security concepts, procedures, security safeguards, practices, guidelines, information security governance, risk management approaches, awareness and training, regulations and assurance to protect the cyberspace environment and critical information assets in Botswana. The specific business problem is policymakers, academia, ICT industry professionals, and members of the public have limited understanding and awareness of cybercrime and cybersecurity.

3. Purpose Statement

The purpose of this qualitative multiple case study was to explore policy frameworks developing countries use to guide the development of cybersecurity policy and strategies organizations use to safeguard and combat cybercrime to protect critical information assets. The target population of this study consisted of 15 managers from University of Botswana, Ministry of Transport and Communications, and Botswana Communications Regulatory Authority in Gaborone.

The outcome of this study may contribute positively to the enhancement of cybersecurity posture in Botswana ensuring the protection of critical information assets. The outcome of this study may also equip security professionals with new strategies, standards, best practices, tools, and techniques essential for effective countermeasures against cybercrime**.**

4. Research Question

RQ: What is the degree to which organizations in Botswana have protected their critical information infrastructure assets from cybercrime?

4.1. Interview Questions

1. What security controls and tools does your organization use to identify, detect, protect, respond to, and recover from incidents of cybercrime?
2. To what degree can adversaries affect the confidentiality, integrity, and availability of your organisation’s computer networks and information assets?
3. To what extent can hackers remotely exploit the vulnerability of your computer network resources?
4. What policy guideline has your organization adopted to safeguard computer networks and information assets from cybercrime?
5. What strategies does your organization use to recruit cybersecurity professionals?
6. What additional information can you provide to help me understand the cybersecurity strategies your organization use to protect critical information assets?

5. Methodology

To address the problem outlined above, I conducted a qualitative multiple case study to establish the extent to which organizations in Botswana are aware of the degree to which cybercrime permeate ICT networks to cause harm on critical information assets in Botswana. I supported the central research question with a few interview questions to establish if organizations in Botswana have adopted or are planning to adopt policy guidelines to safeguard computer networks and information assets from cybercrime.

Interview questions, which I administered through a focus group comprising senior managers from a number of government institutions and the private sector were also aimed at establishing whether managers of organizations in Botswana use any specific methods and techniques to identify, detect, protect, respond, and recover from incident of cybercrime. Participants were also asked whether there are strategies that organizations in Botswana use to recruit cybersecurity professionals. I used Global Cybersecurity Index model developed by ITU in 2007 as a conceptual framework for guiding the study during the review of literature.

6. Literature Review

6.1. Definitions of Cybercrime

A lack of commonly agreed definition of cybercrime and cybersecurity resulted in different jurisdictions and entities defining the terms cybercrime and cybersecurity differently. The U.S. Department of Justice defines computer crime as "any violations of criminal law that involves a knowledge of computer technology for their perpetration, investigation, or prosecution" [39]. The UK Association of Chief Police Officers defines cybercrime as the "use of networked computers, telephony or Internet technology to commit or facilitate the commission of crime" [39].

The Australian Centre for Police Research (ACPR) defines cybercrime as "offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence" [39]. Researchers defined cybercrime as abuses and misuses of computer systems or computers connected to the Internet, which result in direct and/or indirect criminal activity and losses facilitated via the Internet" [32:121].

The National Cybersecurity Policy Framework of South Africa defines cybersecurity as "the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them" [9, December 4, 2015;14].

The term cybersecurity summarizes various activities such as tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, awareness and training, best practices, assurance, and techniques that organizations can use to protect the cyber environment and information assets [13;19].

6.2. Types of Cybercrime

The ICT industry identifies cybercrime in four categories (a) internal computer crimes, (b) telecommunications crimes, (c) computer manipulation, and (d) traditional theft of hardware and software as shown in Fig.1.

6.2.1. Internal computer crimes

Internal computer crimes include Trojan horses, logic bombs, trap doors, computer worms, and viruses. A Trojan horse or Trojan is a type of malware that manifests itself as a legitimate software [21;22]. Kaspersky

Lab indicated that cyber-thieves and hackers often deploy Trojans to gain access to users' systems.

According to Kaspersky Lab, Trojans may sit quietly in a computer, collecting information or setting up holes in the security of the computer network, or they may just take over your computer and lock you out. Once activated, Trojans enable cyber-criminals to spy on computer networks, steal sensitive data, and gain backdoor access to computer systems. Such actions can include (a) deleting data, (b) blocking data, and (c) modifying data, copying data, and disrupting the performance of computers or computer networks.

Researchers define a computer virus as a program that infects other programs by modifying them to make a copy of itself, where every program that is infected also acts as a virus and the infection grows and propagates through computer networks [2;21;22].

Viruses can propagate within a single computer, or may travel from one computer to another using human transported media such as USB flash drive, CD-ROM, DVBD-ROM, or other storage media. Computer worms share several characteristics with viruses [2].

Like viruses, computer worms are self-replicating too, however, worms are standalone and do not rely on other executable code. According to [2], a logic bomb is a code that consists of two parts (payload and trigger) inserted into existing code.

While a payload can be anything that has a connotation of having a malicious effect, a trigger could be design to be set off remotely to set off the absence of an event.

6.2.2. Telecommunication crimes

Law Enforcement Agencies in Botswana need to develop knowledge, skills, and capacity to detect the current and emerging forms of criminology involving telecommunications systems, as they are increasingly becoming targets of criminal activity (see Fig. 1).

Researchers [10] identified a significant trend in the forms of criminology in telecommunications systems largely including theft of telecommunication services, criminal conspiracies, theft of intellectual property, dissemination of offensive materials, electronic money laundering, electronic vandalism, telemarketing fraud, and illegal interception of telecommunication services, to mention but a few.

6.2.3. Computer manipulation crimes

Computer manipulation refers to the use or manipulation of a computer to perpetrate a crime. As shown in Fig. 1, computer fraudsters input into a computer (a) false or misleading data to achieve a specific criminal purpose, (b) manipulating the output of a computer by using a stolen bank account number to make unauthorized withdrawals, or (c) using a computer to create a fraudulent document using a computer.

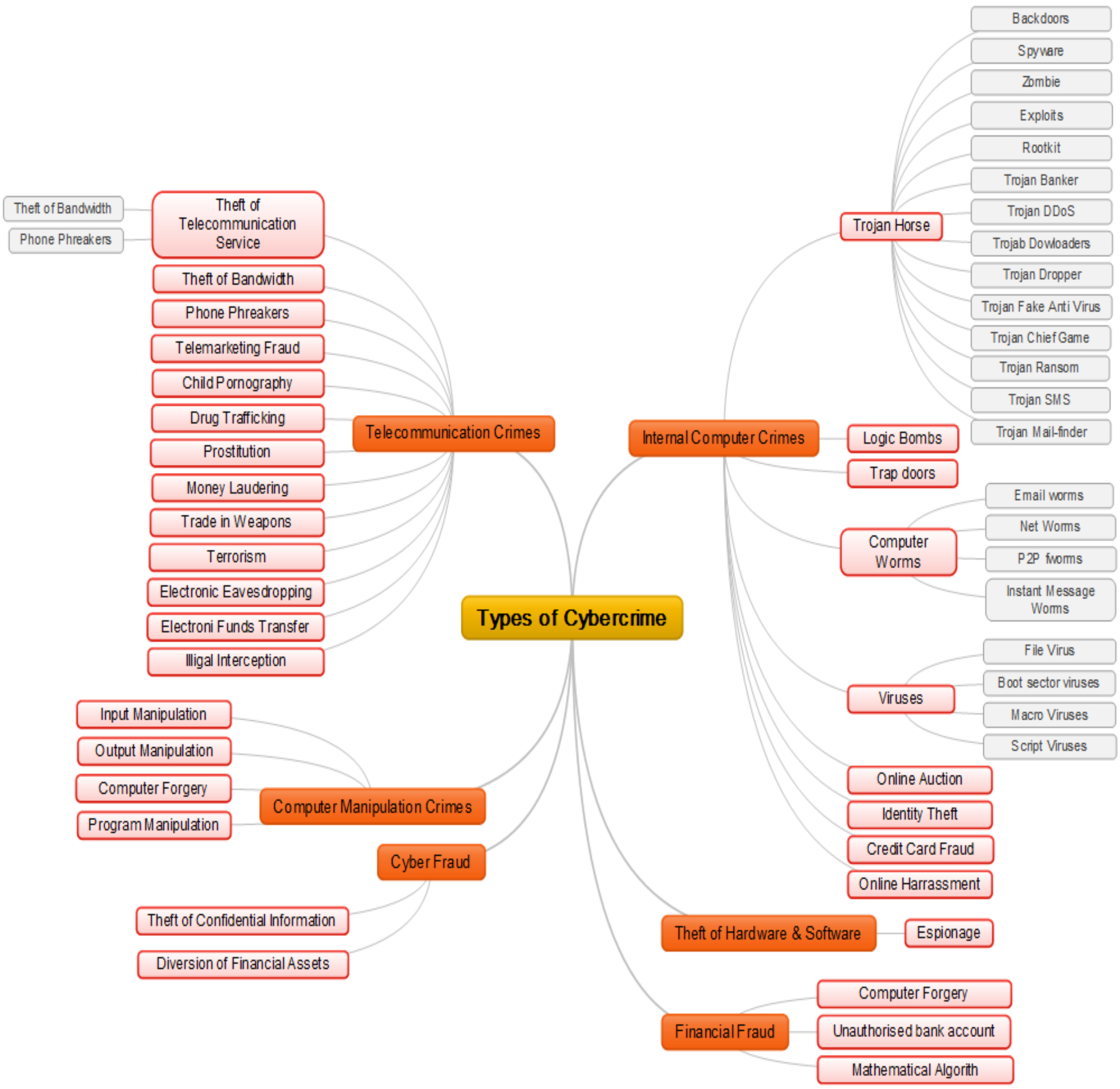

Figure 1: Types of cybercrime

6.3. Types of Cybercrime Attacks

Cyber threats are not only evolving and increasing at an alarming rate, but they also do not recognize borders, hence have the potential to cause devastating consequences in developed and least developed countries alike. Increasing number of wireless devices are abused for illicit cybercriminal activities, including malicious attacks, computer hacking, data forging, financial information theft, online bullying/stalking, and so on [43].

Depicted in Fig.2 are top 10 most common cyberattacks that criminals often use in the cyberspace to compromise security, cause harm or steal sensitive information in computer networks.

According to [7], hacktivists range from teenagers, freedom fighters, disgruntled employees to criminal enterprises or state sponsored undertakings with diverse motives to commit variety of cybercrimes including those identified in Fig. 2.

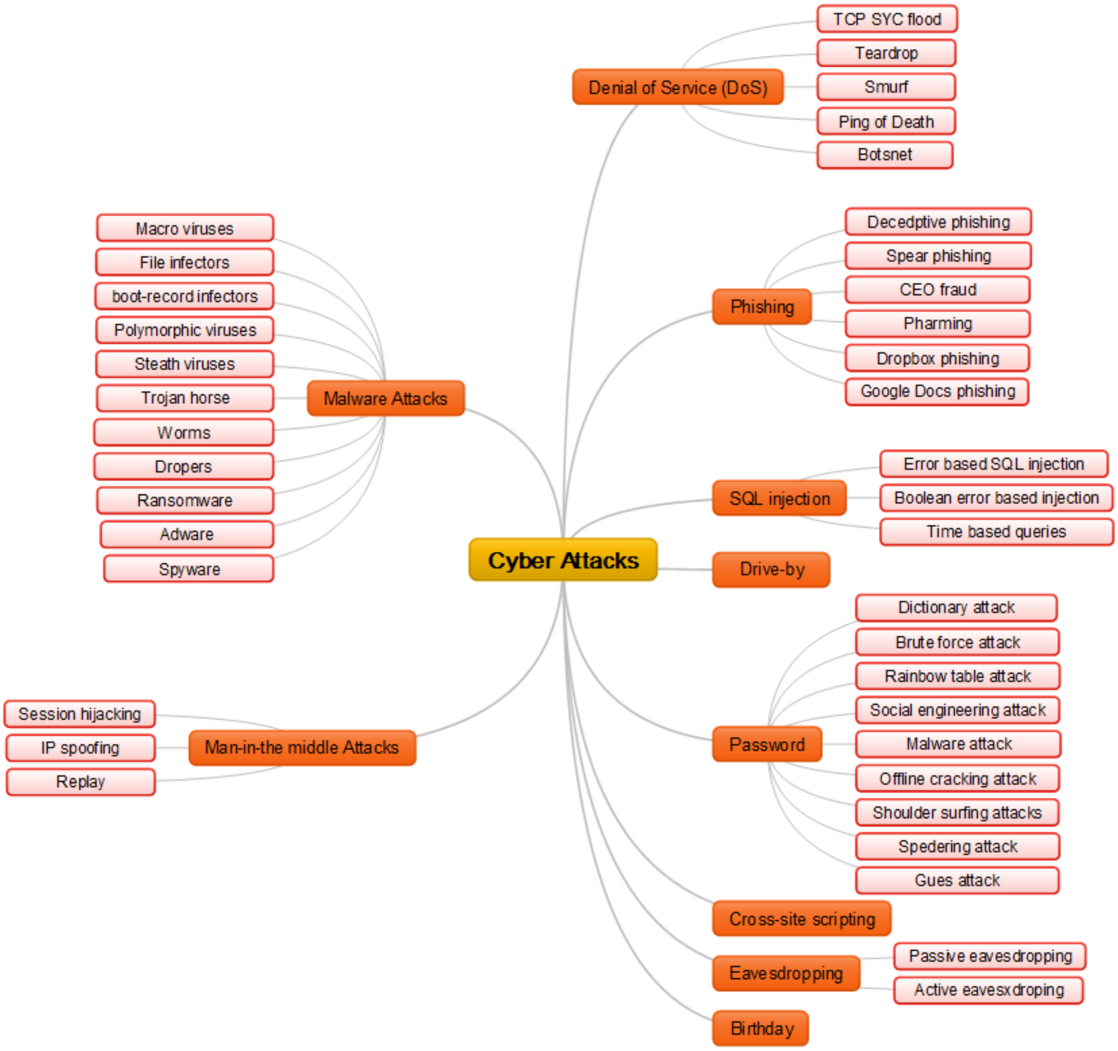

Figure 2: Types of cyber attacks

6.3.1. Combating Cybercrime in Botswana

Botswana recorded 12 cases of cybercrime relating to pornography, website defacement, ransomware, cyber scams/fraud and threatening emails between 2015 and July 2017. The Botswana Police Service however, were of the view that there must be much more cases of cybercrime including cloning of automatic teller machines (ATMs) that victims did not report during the same period. In Feb 2017, hackers gained unauthorized access to the University of Botswana (UB) website and defaced the brand banner with an image of a *Guy Fawkes* mask associated with a hacker group known as *Anonymous*. In May 2017, the Ministry of Transport and Communications (MTC) caused a deliberate shutdown of the Botswana Government Data Network (GDN) due to the WannaCry virus, which threatened to have affected all government offices connected to Government Data Network (GDN). Services that were shutdown included the Immigration and Passport Control services and Court Records Management, Hospital Patient Management System, Citizen National Registration system, etc.

6.3.2. Cyber-attacks in South Africa

South Africa, like most other countries in Africa does not have the necessary capacity to comprehensively deal with cybersecurity. I discussed cybercrime incidences recently recorded in South Africa as follows:

Gautrain incident: Computer-related theft/fraud committed by a group of persons. There was insider collusion with IT persons working for the same company. Value of potential loss was in the region of ZAR800 Million. Computer Forgery refers to the act of unlawfully inserting, altering or deleting computer data or restricting access to the data, to acquire a different evidentiary value in the course of legal transactions [28]. computer fraud involves the manipulation of a computer, by whatever method, in order to dishonestly obtain money, property or some other advantage of value or to cause loss [28].

Eskom incident: Attempted computer-related theft/fraud committed by a group of persons. There was insider collusion with IT persons working for company. Value of potential loss was in the region Value of potential loss ZAR3.5 billion.

Telesure incident: Relates to ransomware. Potential loss in the region of ZAR20 million perpetrated by a group of persons. Various incidents of phishing; DDOS attacks and crypto extortion also took place in South Africa. The South African Police worked closely with the affected parties to investigate the incidents and achieved arrests in the Gautrain, Eskom, and Telesure incidents. The South African Police Service, however, were less successful in the investigation of the less serious cases. In the Telesure incident, actors from outside the country were involved and have not yet been apprehended.

6.3.3. Cyber-attacks in Nigeria

According to [27], major Cyberattacks taking place in Nigeria are ransomware attacks, cyber Ponzi schemes, and the most commons ones being social engineering attacks conducted via email spoofing, SMS and calls. At a cybersecurity meeting in Lagos organized by Price Water House Coopers (PwC) it was discussed that the number of high profile security breaches were growing each year. Cyber criminals to concentrate more on Operational Technology (OT) and the IT environment of an organization to gain unauthorized access to an organization’s data. The experts have also discovered two major new vulnerabilities related to mobile devices being Man-in-the-Disk, which attacks Android applications exploiting a shortcoming in the way that Android applications use storage resources.

In 2016, the most common cyber incidents that took place in Nigeria were botnet attacks as well as command and control systems from a foreign country, which used infected systems (zombies) in Nigeria to attack systems in other countries. Nigeria was able to find out who perpetrated the incident by carrying out investigation in conjunction with the affected country and engaging the Internet service provider (IS) in Nigeria with the relevant information of the date and time of the attack to get to know command and control system and the zombie involved. For this botnet incident, the command and control system was located outside Nigeria while the individual bots (zombies) resided within Nigerian borders. In 2017, Nigeria was affected by the WannaCry ransomware, which crippled many IT departments of organizations in the country.

6.3.4. Cyber-attacks in the Democratic Republic of Congo

National authorities report that the hacking of electronic mailboxes and the dissemination of false information on social networks was atop the list of cyber incidents, the officials also pointed out that it was difficult to know whether the perpetrators of the incidents were located within or outside of the country.

6.3.5. Cyber-attacks in Mozambique

According to Mozambican Communications Institute, over two hundred cyberattacks have been registered in just two years between 2016-2017, affecting both private companies and public entities. Mozambique is one of the least developed countries in terms of cybersecurity.

6.3.6. Cyber-attacks in Rwanda

At least eight million cyberspace attackers attempted to hack into Rwanda's financial institutions in 2017 and in several occasions managed to enter into one of the systems, however, the stolen money was always tracked and recovered.

Significant Cybercrimes:

- Central Bank Governor John Rwangombwa said the bank registered 80 hacking cases. One case of money recovered was successfully done with the help of some Rwandans in one of the institutions in which Rwf900million was stolen.
- Again Last year, hackers known as 'Anonymous' managed to enter the security of a one company Broadband Systems Corporation (BSC), a private firm that provides the government with video conferencing technology and dumped its private data to the public.
- In 2016, Police says that Rwanda managed to intercept attempts to steal Rwf1billion and €340 while in 2017 the cyber thieves attempted to walk away with Rwf2billion and $ 605,028 in vain.

While both the bankers, police and the central bank agree that cybercrimes are a new phenomenon in the country, Rwanda has made a commitment to beefing up IT equipment in banks, training staff in hacking loophole and attempts and sensitize citizens- with the latter being a priority this year and due to start soon.

7. Overview of Global Cybersecurity Index (GCI)

Cybersecurity is a complex challenge that embraces good governance, policy, strategic, technical, and legal aspects for societal good [13]. Combating cybercrime requires a systematic and collective implementation of the Global Cybersecurity Agenda to drive the Global Cybersecurity Indices, which ITU periodically measures using GCI measurement pillars: legal, technical, organizational, capacity building, and International cooperation discussed below. Delivering an effective cybersecurity program requires a systematic application of management policies, procedures, and practices aimed at identifying, analysing, evaluating, and monitoring risks affecting organizations.

7.1. Legal measures

Although the Botswana government first enacted Cybercrime and Computer Related Crimes Act in 2007, which was reviewed in 2018, the legislation does not explicitly address legal challenges as prescribed under the Global Cybercrime Index Model. The Botswana government enacted legislations and regulations laws on Data Protection, Electronic (Evidence) Records Act, 2014, and Electronic Commerce and Signatures, which [11] suggested they have not been effective in addressing cybercrime and cybersecurity. African countries' push for socioeconomic growth through advanced ICTs, little interest developed in creating appropriate policies and laws to govern the collection, use, storage, and dissemination of data [38].

Effective legal measures organizations use to address cybercrime and cybersecurity include the implementing of cybercriminal legislation, cybercriminal regulation, and cybercriminal training as herein under discussed [30;37]. Likewise [4] posited that African countries should take adequate measures to ensure their criminal and procedural laws meet the challenges posed by cybercrime. In 2009, the International Telecommunications Union underscored that the "legal measures focusing on how to address the legislative challenges posed by criminal activities committed over ICT networks" (10:13).

7.1.1. Cybercriminal legislation

Legislative instruments developed to support the national cybersecurity strategy include among other laws: (a) Cybercrime and Computer Related Crimes Act No. 22 of 2007, (b) Communications Regulatory Authority Act No. 19 of 2012, (c) Electronic communications and transactions Act No. 14 of 2014, (d) Electronic communications and transactions regulations [30], of 2016. Defining "cybersecurity law requires an examination of the harm that the law seeks to prevent and understanding those harms is essential to prioritizing the goals, limits, and scope of cybersecurity law" [15:989]. The development of Botswana National Cybersecurity Strategy [25], among other important goals, aims at (a) making Botswana more secure and resilient to cyberattacks, (b) building cybersecurity capacity and capability in Botswana, (c) raising and promoting cybersecurity awareness among the general public, (d) fostering cybersecurity research and development, (e) enhancing collaboration and cooperation on cybersecurity issues at national and international level, and (f) harnessing or leveraging Botswana's cyberspace for socioeconomic development [3]. Despite the enactment of these legal instruments, a cybercrime and cybersecurity policy framework is yet to be developed [1;5]. As financial sectors are highly interconnected and provide products and services that are highly vulnerable to cyberattacks, formulation and enforcement of national policies or frameworks for strengthening cybersecurity has increased substantially [5].

7.1.2. Cybercriminal regulation

While cybercrime is a major concern for most organizations, only a handful of jurisdictions in Sub Saharan

Africa have specific regulatory initiatives to address cyber risks [5]. While regulations and compliance measures focused on law on data protection, electronic records Act, 2014, and electronic commerce and signatures, regulations and compliance specifically dealing with cybercrime and cybersecurity have not been developed in Botswana. Regulation makes issues more visible to boards of directors and executive leadership, regulation on cyber risk gives banks stronger incentives to invest in improved cybersecurity environment than it would be the case in other sectors of the economy [5]. Thus, the regulatory framework on cybersecurity should be explicit on information security policy in public sectors, providing information security direction and driving the implementation of national incident responses Centre (CERT). The regulatory framework should also emphasize the development of personal data protection Act to safeguard personal data and privacy.

7.1.3. Cybercriminal training

As suggested by [18], when formulating a cybercriminal training syllabi, policymakers, academia, regulators, and ICT industry professionals must collectively agree on achieving a minimum of the following lifelong learning outcomes:

- Defining the nature and scope of cybercrime
- Developing knowledge of major incidents of cybercrime and resulting impact
- Analysing the national and global digital law enforcement efforts
- Critically considering specific laws and policies governing cyber detection and prosecution
- Identifying and evaluate the specific technology that facilitates cybercrime and digital law enforcement
- Critically evaluating the impact of cybercrime on information assets

The U.S. Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS) is the premier online resource for cybersecurity training [11], which Botswana may consider a benchmark and emulate in an effort to enhance awareness, education, and training on cybercrime and cybersecurity. Developing strategies ICT managers may use to build cybersecurity competencies among employees is essential [34].

7.1.4. Technical and procedural measures

The technical and procedural measures of the GCA promote the adoption of enhanced approaches of improving security and risk management in cyberspace, including accreditation schemes, protocols and standards [10; 12]. Critical elements of the technical and procedural pillar of the GCA/GCI framework include developing cybersecurity incidents response teams at national, government, and sectoral levels as well as developing relevant standards for detecting cybercrime affecting organizations. Without adequate technical capabilities to detect and respond to cyberattacks, nation states remain vulnerable. Effective ICT development and use can only truly prosper in a climate of trust and security. Nation states therefore need to establish accepted minimum security criteria and accreditation schemes for software applications and systems

7.1.5. National, government, and sectoral CIRTs

As nations continue to develop their national, government, and various industry sectoral cyber incidents response teams (CIRTs), and security operations centers (SOC), Botswana Communications Regulatory Authority (BOCRA) has taken the role of building a national CIRT. In 2012, ITU-D conducted a CIRT readiness assessment for Botswana at Maseru, Lesotho in October, where the outcome of the assessment was Botswana does not have an officially recognized national CIRT [15]. A computer emergency response team (CERT) plays an important role in the technical aspect of implementation to detect attacks against the organization [42]. The Ministry of Transport and Communication (MTC) in consultation with BOCRA and relevant stakeholders is in final enactment stage of National Cybersecurity Strategy by Parliament.

The Botswana National Cybersecurity Strategy clarifies roles various stakeholders need to play and outlines action plan to safeguard the country against incidents of cybercrime. According to [11;12;13] the fundamental role of government in the fight against cyber threats is among others to (a) ensure the continuity of society in time of crisis, (b) protect essential services and critical national infrastructure, restore control of information dissemination, train personnel as responders, and recover a state of normality quickly. The outcome of a CIRT readiness assessment conducted by ITU-D for Botswana in 2012, revealed Botswana does not have officially recognized national and sector specific cybersecurity frameworks for implementing internationally recognized cybersecurity standards (11;12).

7.2. Organizational structures

The pillar of organizational structure include generic frameworks and response strategies for “prevention, detection, response and crisis management of cyberattacks, including the protection of critical information infrastructure systems” (23:20). Organizational structure measures that assist organizations detect, prevent, protect, respond, and recover critical information infrastructure include developing and executing national cybercrime strategy, identifying and engaging responsible agencies and implementing compelling cybersecurity metrics.

7.2.1. Cybercrime strategy

To develop and sustain a coherent approach of cybersecurity, it is imperative that a national strategy, enforceable at a national level exists and executed. The development of Botswana National Cybersecurity Strategy anchors on the National Broadband Strategy, which underpins constituents of the legal framework including electronic commerce and signature, consumer protection, protection of personal data, cybercrimes, security of systems and networks, and infrastructure development and usage [2;25]. For the National Cybersecurity Strategy to be effective, it needs to reflect the cybersecurity posture of the country. An analysis of the country’s existing cybersecurity strengths and weaknesses should be conducted, and relevant materials and documents should be consulted in collaboration with relevant stakeholders across government, private sector and civil society.   Additional to the overall cybersecurity direction, vision, scope and a set of objectives to be accomplished within specific timeframe, the strategy has to define and confirm the mandate of the different entities responsible for initiating and developing cybersecurity policies and regulations within the country.

7.2.2. Cybersecurity metrics

Information security and risk management leaders should consistently report to the board of directors and executive management the following: regulatory updates, risk management program, vendor and third party service provider management, IT budget considerations, security monitoring and testing reports, incident management, and training activities.

7.2.3. Cybersecurity capacity building

Investing in building the capacity of employees could earn the organization lusting reputation and protection from cybercrime. Researchers [8] refer to cybersecurity capacity building as a set of initiatives that empowers individuals, communities, and governments to reap gains from investments in digital technologies. Organizations need to collectively engage cybersecurity experts “to setup computer security incident response teams to provide support in developing national cybersecurity policies and strategies and carryout awareness campaigns with the view to reap potential gains from investments in digital technologies [8: para 2]. As skilled cyber actors exploit vulnerabilities in computer networks to steal information and develop capabilities to disrupt, destroy, or threaten the delivery of services, organizations need to adopt a consistent approach for change management and restructuring in view of cybersecurity standards [31]. To achieve this milestone, organizations should develop a dedicated budget for cybersecurity awareness through focused group forums and planned campaigns [12].

7.2.4. Intra agency and international cooperation

Sub-Sahara Africa countries need to ratify and comply with conventions such as European Convention on Cybercrime and United Nations Conventions against Transnational Organized Crime. The conventions encourage countries to combat cybercrime based on harmonized and streamlined international laws [5]. The European Convention on Cybercrime is “the first international treaty on crimes via Internet and other computer networks, which addresses infringements of copyright, computer related fraud, child pornography, and violations of network security” [5:126]. To remove obstructions in the handling of Internet fraud, telecommunications fraud, cybercrime and computer related crimes, cooperation and communication between the different law enforcement agencies, policymakers, regulators, academia, and ICT industry professionals need to promote and strength inter-agency coordination [24]. Based on this understanding, law enforcement agencies in Botswana, especially Botswana Police, Directorate of Intelligence and Security, as well as Financial Intelligence Agency should establish databases of Internet fraud, telecommunications fraud, cybercrime and computer related crimes to allow data sharing and big data analysis of such information with the view to determine how perpetrators would reengage in criminal activities.

8. Combating Cybercrime in Botswana

The absence of policy framework and a lack of appropriate cybersecurity framework to combat cybercrime at national level compounds cybersecurity challenges in Botswana. According to [6] organizations may categorize cybersecurity challenges into (a) limited visibility, (b) socio-technological complexity, (c) ambiguous impact related to strong incentives of market parties, and the contested nature of fighting cybersecurity. South Africa published the National Cybersecurity Policy Framework (NCPF) as approved by the Cabinet on March 7, 2012. The NCPF addresses (a) cybersecurity threats, (b) establish Cybersecurity Response Committee chaired by the State Security Agency (SSA), (c) coordinate resources in the achievement of common cybersecurity safety and security objectives, and (d) promotion of cybersecurity measures by all role players including state, public, private sector, and civil societies [8]. Nonetheless, Botswana, Kenya, Uganda and Cameroon have also taken steps to introduce cyber legislation and build regional partnerships to combat cybercrime.

Researchers and scholars in the ICT industry identify cybercrime in four categories (a) internal computer crimes, (b) telecommunications crimes, (c) computer manipulation, and (d) traditional theft of hardware and software. Internal computer crimes include attacks such as Trojan horses, logic bombs, trap doors, computer worms, and viruses. A significant criminology trend in telecommunications systems largely including theft of telecommunication services, criminal conspiracies, theft of intellectual property, dissemination of offensive materials, electronic money laundering, electronic vandalism, telemarketing fraud, and illegal interception of telecommunication services [7], which many developing countries cannot detect nor prevent from occurring.

Hackers represent cybercrime attacks or threats, which manifest themselves in various forms including password, malwares, denial-of-service, phishing, man-in-the middle, and structured query language (SQL) injection. Obtaining unauthorized access to computer systems using numerous tactics such as brute force attacks, malware attacks, dictionary attacks, rainbow table attacks, social engineering attacks, or office cracking attacks allows hackers to steal information or cause harm to information infrastructure assets. Malware attacks constitutes spyware, adware, ransomware, and many other malicious software that cause harm and losses to businesses today [41]. Spyware as a software is usually designed to gather data (e.g., passwords, PINs, credit card numbers, monitoring key strokes, browsing habits, and harvesting email addresses) from computers or other devices for a third party without the consent or knowledge of the user [20;21]. Ransomware or crypto virus is the new form of threat in the cyberspace recently known to be damaging company reputations and eroding Internet consumer confidence. Losses incurred in 2016 due to ransomware exceeded US$1bn globally [3]. Ransomware makes a bitcoin wallet per victim and payment in the form of digital bitcoins in the dark web, which utilizes the anonymity network [36;41].

Cyber threats are not only evolving and increasing at an alarming rate, but they also do not recognize borders, hence have the potential to cause devastating consequences in developed and least developed countries alike. Nikolova (2017) posited that the most common cybersecurity threats are identity theft, theft of sensitive information, theft of intellectual property, cyber vandalism, phishing, and distributed dial of service (DDoS) attacks. Cybercrime activities include hacking, cyber stalking, virus dissemination, dissemination of obscene material/pornography, cyber terrorism, cyber defamation, online fraud and cheating, phishing, e-mail spoofing, forgery, data diddling, salami attack, Internet time thefts, and Trojan horse [35].

While improvements in global telecommunication infrastructure, including computers, mobile phones, and Internet facilities, enabling access from anywhere, anytime in the world have brought about major transformation in world communication [8], such developments have also substantially increased the cyber warfare in the cyberspace. Differences in Internet penetration, technological development, private sector dynamics, government policies and strategies, means cybersecurity continues to emerge from bottom up [17]. Resources that support critical functions and related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Conventional organized crime groups are increasingly involved in cybercrime, where attacks are carefully planned and executed by skilled individuals [40].

Between 2015 and July 2017, Botswana recorded over 12 cases of cybercrime relating to child pornography, website defacement, ransomware, cyber scams/fraud and email phishing. Hackers defaced several Websites in 2016 and 2017 including Sunday Standard Newspaper, Botswana Fibre networks, and a few other institutions. In February 2017, hackers defaced the University of Botswana (UB) website replacing the top UB brand banner with an image of Guy Fawkes mask associated with a hacker group known as Anonymous.

9. Conclusion

In addressing the study research questions, I used GCI model to assess Botswana's readiness in combating cybercrime in terms of performance measures of legislations, technical, organisational structures, capacity building, and intra-agency and international cooperation. While Botswana has achieved tremendous growth in ICT infrastructure development, major challenges still remain in developing human capital in terms of knowledge, skills, and abilities to fight cybercrime. The development of appropriate policies and strategies to fight cybercrime and protect national information infrastructure assets is also lacking. Policymakers, the academia, and ICT industry professionals are now willing to work together to achieve a common goal in securing critical information assets. While awaiting the development of national cybersecurity policy and approval of national cybersecurity strategy, government should be proactive in driving cybersecurity awareness and training to reduce the consequences of cyber-attacks. Law enforcement agencies, policymakers, regulators, academia, and ICT industry professionals should play a leading role in promoting and strengthening inter-agency coordination of computer incidents and security operations strategies.

References

[1]. Akuta, E, A-M, Ong'oa, I. M., Jones, C. (2011, March). "Combating cybercrime in Sub Saharan Arica: A discourse on Law, Policy, and Practice". Journal of Peace, Gender, and Development Studies, 1(4), p. 129-137. Available: http://www.interesjournals.org/JPGDS [October 5, 2018].

[2]. Aycock, J. (2006). Computer Viruses and Malware. Springer Sciences and Business Media, LLC. New York. Available: https://link.springer.com/content/pdf/bfm%3A978-0-387-34188-0%2F1.pdf [February 10, 2019].

[3]. Botswana Communications Regulatory Authority (2013). "Botswana National Broadband Strategy". Available: http://www.bocra.org.bw/ [October 13, 2018].

[4]. Brewer, R. (2016). "Ransomware attacks: Detection, prevention, and cure". Network Security Journal, 9, p. 5-6. doi.10.1016/S1353-4858 (16) 30086-1 [November 2018].

[5]. Cassim, F. (2011, January). "Addressing the growing spectre of cybercrime in Africa: Evaluating

measures adopted by South Africa and other regional role players". First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011. Available: https://core.ac.uk/ [October 21, 2018].

[6]. Crisanto, C., and Prenio, J. (2017). "Financial stability institute insights on policy implementation No. 2: Regulatory approaches to enhance banks' cybersecurity frameworks". Available: https://www.bis.org/ [November 12, 2018].

[7]. De Bruijn, H., & Janssen, M. (2017). "Building cybersecurity awareness: The need for evidence-based framing strategies". Government Information Quarterly, 34, p. 1-7. doi.10.1016/j.giq.2017.02.007 [October 25, 2018].

[8]. Ekoa, R. & Mungwe, M. (2018, May). "A review of cybercrime in Sub Saharan Africa: A study of Cameroon and Nigeria". International Journal of Scientific & Engineering Research, 9(5), p. 211- 228. Available: https://www.ijser.org/researchpaper [October 26, 2018].

[9]. Government Gazette No. 39475 (December 4, 2015). "The National Cybersecurity Policy Framework: State Security Agency". Retrieved from https://www.gov.za/ [October 18, 2018].

[10]. Grabosky, P. N., Smith, R. G., & Wright5, P. (1996). "Crime and Telecommunications No. 59 Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice". Available: https://aic.gov.au/publications/tandi/tandi59 [October 1, 2019].

[11]. Hohmann, M., Pinrang, A., Benner, T. (2017). "Advancing cybersecurity: Implementing a principles-based approach". Available: http://www.gppi.net/publications/data-technology politics/article/advancing-cybersecurity-capacity-building-implementing-a-principle-based-approach [December 13, 2018].

[12]. Homeland Security (2017). "Cybersecurity training and exercises". Available: https://niccs.us-cert.gov/ [November 23, 2018].

[13]. International Telecommunication Union – Development Sector (2009). "Understanding cybercrime: A guide for developing countries". Available: https://www.itu.int/ITU-D/cyb/cybersecurity [January, 16, 2019].

[14]. International Telecommunication Union – Development Sector (2017). "Global Cybercrime Index, 2017". Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [January, 18, 2019].

[15]. International Telecommunication Union – Development Sector (2013). "Cyberwellness profile: Botswana". Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Botswana.pdf [January, 18, 2019].

[16]. International Telecommunication Union – Development Sector (2014). Global cybersecurity index and cyber wellness profiles. Available: https://s3.amazonaws.com/academia.edu [January, 16, 2019].

[17]. International Telecommunication Union – Development Sector (2015). "Global cybersecurity index and cyber wellness profiles". Available: https://s3.amazonaws.com/academia.edu [December 18, 2018]

[18]. International Telecommunication Union – Development Sector (2017). Global Cybercrime Index, 2017. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[19]. International Telecommunication Union – Development Sector (2018). "Guide to developing national cybersecurity strategy: Strategic engagement in cybersecurity". Available:

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf [January, 18, 2019].

[20]. International Telecommunication Union (2018). ITU/BDT Security Programme: Global Cybersecurity Index Reference Model Ver. 1. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv3 [March 28, 2019].

[21]. Kaspersky Laboratories (2018). "What is a Spayware?" Available: https://usa.kaspersky.com/resource-center/threats/spyware [January 2019].

[22]. Kaspersky Laboratories (2018). "What is a Trojan Virus?" Available: https://www.kaspersky.com/resource-center/threats/trojans [January 15, 2019].

[23]. Kosseff, J. (2018). "Defining cybersecurity law". Available: https://ilr.law.uiowa.edu [October 12, 2018].

[24]. Lin, L.S.F. (2018). "An emerging global security threat: Internet and telecommunication fraud crime and Taiwan's response". Available: https://www.diplomaticourier.com/an-emerging-global-security-threat-internet-and-telecommunication-fraud-crime-and-taiwans-response [October 26, 2018].

[25]. Ministry of Transport and Communications (2016, September). "Draft Broadband Strategy". Available: http://www.uasf.org.bw/wp-content/uploads/2016/10/Draft-National-Broadband-Strategy.pdf [March 28, 2019].

[26]. Morgan, S. (2016). "Cybercrime Costs Projected to Reach $2 Trillion by 2019" Available: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4b5c74163a91 [October 25, 2018].

[27]. Muhammad, S. I., & Kiru, M. U. (2017) "A situational analysis on cybercrime and it economic impact in Nigeria". International Journal of Computer Applications 169(7), p. 19-29. doi: 10.5120/ijca2017914788. [March 5, 2019].

[28]. Mungwe, R. E. M. (2018). "A review of cybercrime in Sub Saharan Africa: A study of Cameroon and Nigeria". International Journal of Scientific & Engineering Research, 9(5), p. 211-228. Available: https://www.ijser.org/researchpaper [January 17, 2019].

[29]. National Institute of Standards and Technology (April 16, 2018). "Framework for Improving Critical Infrastructure Cybersecurity" [January 2017]. doi:10.6028/NIST.CSWP.0416218 [December 14, 2018].

[30]. Newell, B. (2017). "Cybercrime and digital law enforcement". Available: https://ci.uky.edu [February 5, 2019].

[31]. Nikolova, I. (2017). "Best practice for cybersecurity capacity building in Bulgaria's public sector". Information & Security, 38, p. 79-92. doi:10.11610/isij.3806 [February 26, 2019].

[32]. Osho, O., & Onoja, A. G. (2015). "National cybersecurity policy and strategy of Nigeria: A qualitative analysis". International Journal of Cyber criminology, 9, p. 120-143. doi: 10.5281/zenodo.22390 [November 21, 2018].

[33]. Perche, P. (2017). "Cybersecurity needs to be seen as strategic issue, not just an IT investment. Fortinet". Available: https://www.fortinet.com/blog/business-and-technology/report-cybersecurity-needs-to-be-seen-as-a-strategic-issue-not-just-an-it-investment.html [October 23, 2018].

[34]. Rabogadi, T. A. (2017). “Strategies information and communication technology managers use to build employee competencies”. Doctoral dissertation, Walden University, 2017, United States of America. Available: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=5067&context=dissertations [September 5, 2018].

[35]. Schjolberg, S. (2004). “Computer-related offences”. Available: http://cybercrimelaw.net [November 22, 2018].

[36]. Semboja, H. H., Silla, B. S., & Musuguri, J. N. (2017). “Cybersecurity institutional framework in Tanzania: A policy Analysis”. Global Scientific Journal, 5(6), 13-28. Available: www.globalscientificjournal.com [November, 17, 2018].

[37]. Shiloh, J., & Fassassi, A. “Cybercrime in Africa: Facts and figures, July 7, 2016. Available: https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html [January 10, 2019].

[38]. Sutherland, E. (2018). “Digital privacy in Africa: Cybersecurity, Data Protection, and Surveillance”. Available: https://ssrn.com/abstract=3201310

[39]. Tafazzoli, T. (2018). Cybercrime legislation. Available: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/ [November 10, 2019].

[40]. Tariq, M., A., Brynielsson, J., & Artman, H. (2012). Framing the attacker in organised cybercrime. 2012 European Intelligence and Security Informatics Conference, 30-37. doi: 10.1109/EISIC.2012.48

[41]. Upadhyaya, R., & Jain, A. (2016). “Cyber ethics and cybercrime: A deep delved study into legality, ransomware, underground web and bitcoin wallet”. 2016 International Conference on Computing Communication and Automation (ICCA). doi:10.1109/CCAA.2016.7813706 [February 17, 2019].

[42]. Yokohama, S. (2016). “Cybersecurity for business experts: An NTT publication for top management”. Available: https:/Cybersecurity_for_Business_Executives2.pdf [September 23, 2018].

[43]. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). “A survey on wireless security: Technical challenges, recent advances, and future trends”. Proceedings of IEEE, 104, p. 1727-1765. doi:10.1109/JPROC.2016.2558521 [November 20, 2018].