The International Journal of Multi-Disciplinary Research
ISSN: 3471-7102

Assessment of Cybersecurity and the Law in Zambia

(Conference ID: CFP/171/2017)

Author: Moonde Rodgers
School of Engineering,
Department of Information Security and Computer Forensics,
Information and Communications University, Lusaka Zambia
Email: rodgersmoonde@gmail.com

Abstract
The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. Cybercrime is one of the common seditious practices committed by the computer experts on the cyberspace worldwide. Zambia is no exception and the existing laws are likely to be unenforceable against such crimes. This lack of discreet legal protection means that businesses and governments must solely rely on technical measures to protect themselves from those with intent to steal, deny access to, or destroy valuable information. Rule of Law while essential, is not sufficient to make cyberspace a safe place to conduct business in most developing countries like Zambia. Self-protection, need to be compulsory because countries whose institutions lack adequate protection relational to cybersecurity will become increasingly less able to compete in the new economy. The emergence of new types of crimes as well as the commission of traditional crimes by means of new technologies is likely to be very rampant in Zambia because of inadequate institutional cybersecurity mechanisms. In the current era of online processing, maximum of the information is online and cyber threats are rising. There are a huge number of cyber threats and their behavior is difficult to early detection hence difficult to restrict in their early phases and these cyber-attacks may have some motivation behind them. Cybercrime has serious impact over the society in the form of economical disrupt, psychological disorder, threat to National defense and other areas of development. Moreover, the consequences of criminal behavior can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries. This Paper therefore endeavors to assess the Zambian cyber security context and the law in the pursuit of practical measure provision to mitigate cybercrime.
Keywords*: Cybercrime, Potential Economic Impact, Consumer Trust, National Security, Self-protection.*

ABBREVIATIONS

ACC	Anti-Corruption Commission
BOZ	Bank of Zambia
HARID	Home Affairs Research and Information Development
ICT	Information and Communication Technologies
IT	Information Technology
NATC	National Anti-Terrorism Center
ZICTA	Zambia Information and Communication Technologies

1. INTRODUCTION

1.1 Background

In 2006, the Government of the Republic of Zambia through the Ministry of Communication and Transport formulated the National Information and Communication Technology [1]Policy. The policy recognizes that the world has embraced Information and Communication Technology as an enabler of social and economic development and that the industry is growing exponentially and making significant contribution to global trade and investment.

The policy notes that ICT is receiving focus at various fora as demonstrated by the United Nations Millennium Development Goals (MDGs) and the World Summit on the Information Society (WSIS). Both initiatives resulted in the promotion of information and knowledge based society as the basis for creating wealth. An opportunity arose for Zambia to join the global village by connecting commerce and trade. The policy set the framework for Zambia's participation in the global economy.

The inclusion of ICT in all the sectors was made a priority in national development. Despite the numerous setbacks in the implementation of that policy many institutions (both private and public) especially private sector have set the needful ICT infrastructure and incorporated it in commerce and trade. Nonetheless, there is a significant lack of physical and logical protection of the ICT infrastructure and the information on the computers stands at risk as witnessed by the growing number of cyber-attacks in Zambia as technology continues advancing.

Presently, the Government of the Republic of Zambia has in place legal documents regarding cybersecurity. Unfortunately, they are not adequate considering the complexity and dynamic nature of cybercrime, and the effect thereof to the national economy has been felt tremendously hence the need to consider some workable means of self-defense thereby de-escalating the phenomenon.

1.2 Statements of the problem

There is a continued escalation in the levels of cybercrime in Zambia in both private and public sector despite the existence of security features that ensure control and effective monitoring in some institutions. (Nyati, 2017). Many researches have been conducted to determine the possible causes of cybercrime in areas of: the availability of ICT infrastructure, the adequacy of the law, and awareness. Solutions to these problems have been sought to mitigate the problem but in vain. It is therefore against this background that the researcher sought to carry out a research to determine the Cyber security context in Zambia, find out how the Zambian laws protect the cybercrime victims and

[1] https://thezambian.com/2007/04/06/information-and-communication-technology

to design practical ways of enhancing the effectiveness of cybersecurity in Zambia.

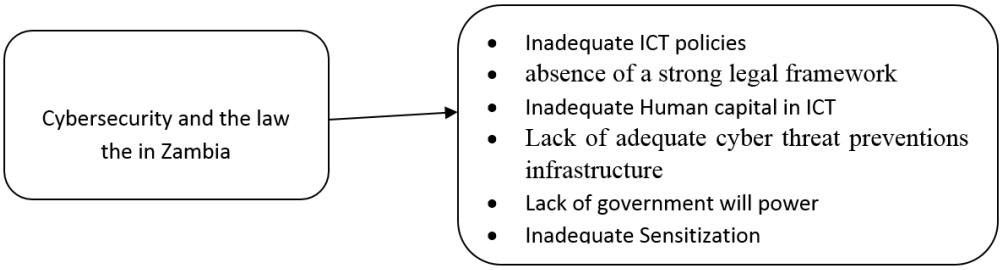
1.3 Objectives of the project

The main objective of the study was to assess cybersecurity and the Law in Zambia. The explicit objectives being:

i. To determine the cybersecurity context in Zambia;
ii. To find out how the Zambian cyber laws protect cybercrime victims in Zambia; and
iii. To find ways of enhancing the effectiveness of cybersecurity in Zambia.
iv.

1.4 Theoretical Framework / Model

This project is theoretically informed by several related literatures that form a compelling interdisciplinary intersection:



1.5 Literature Review

This chapter focuses on many related literature that covers the broad framework from which the research was done. The focus was on the cybersecurity context in Zambia, motivating factors of cybercrime, prevalence thereof and the effects of cybercrime to the national economy. Literature review is the analysis of the book or manuscripts that researchers consulted in understanding and investigating the problem during the research. Awoniyi S.A., Anderanti, R.A & Tayo, A.S (2011). In this context of study, the literature related materials were reviewed to help the researcher have an understanding and insight of the previous researched work.

Dashora (2011), hints that the world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of mankind on these machines. Internet has enabled the use of website communication, email and other forms of information transfer anytime anywhere instigated by the IT solutions herein for the betterment of humankind.

Cybersecurity continues to capture and enthrall people from all walks of life. Musuva-Kigen e tal (2016 pp 37), refers to cybercrime as a criminal activity perpetuated through the use of a computer and in what is commonly referred to as cyberspace. Or the traditional forms of crime committed over elect communication networks and information systems and/or crimes unique to

electronic networks. For instance, attacks against information systems, denial of service and hacking. Cybercrime is emerging as a serious threat worldwide. Governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are seen taking shape.

The fascination in this vector of crime is no different than the reports of any other crime such as robbery, burglary or fraud. The very nature of cyber-crime being in the cyberspace however, appears to provide fodder on which morbidly attracts so many. Africa is no different in falling victim to cybercrime. However, other scholars like Dashora notes that there simply is not enough information out to inform both government and individuals of what specific crimes to guard against as well as how to effectively respond when one falls victim.

Musuva Musuva-Kigen e tal feels that the reason for the perpetuation of cybercrime can be attribute to poverty, adventurism, disgruntled revenge, bad socio-policies, negative/failed religio-cultural norms, and unemployment. The recent launch of cashless policies as well as growing e-business solutions in the country [Zambia] has further exasperated this situation. The lack of adequate cyber threat preventions infrastructure and logistics as well as the absence of a strong legal framework that guarantees timely prosecution of identified cases has further encouraged people to get involved in cybercrime.

Rather than looking at this as a collective problem to be addressed by all, many still see the solution to identify and fight cybercrime as an exclusive preserve of the government. However, it has been found that the biggest source and victim of cybercrime are individuals and corporate entities in the private sector. The private sector has simply not done enough investment in fighting cybercrime. And for this, the government needs to do more in the area of legislative revamp in empowering stakeholders like law enforcement agencies on capacity building, and encouraging synergy amongst the various agencies.

Research grants need to be established for training and empowerment of the public on cybersecurity services. Human resources/capacity building is key, backed up by legal and legislative reviews of the current laws. There is need to understand the cybercrime dynamism developing information technology essential for fighting cybercrime, and closing the loophole between govern agencies. A public-private sector initiative is required to build the intelligence and strategy required to be ahead of the cyber criminals.

A policy document outlining with detection/investigating/prosecuting of cybercrime, protecting trusted communication and safety, security software and hardware requirement and guidelines must be devised. According to the findings of his fascinating survey, Thoithi (2016), observes that cybercrime has been on a steady increase since its debut in reference to their survey back in 2011 in comparison with the 2016 survey.

Thiothi also notes that **the rise of technology has exposed organisations to a number of threats**, the key ones being:

- *Insiders* — not only employees but also trusted third parties with access to sensitive data;
- *Organised crime syndicates* — threats that include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims often include financial institutions, retailers, medical and hospitality companies; and
- *Hacktivists* — threats include service disruptions or reputational damage; victims often include high-profile organisations and governments.

Thoithi highlights that the nature of cybercrime is such that the threat actors can target any country in the world, regardless of their own location. This means that whether or not the cybercrime threat exists within Zambia and Zambia is at risk. Their survey results show that cybercrime increased by 23% in Zambia (from 22% in 2014 to 27% in 2016), a trend which we are seeing globally.

In his garish report, Musuva-Kigen e tal (2016 pp 52, 62) notes two main initiateves in enhancing the effectiveness of cybersecurity: *Collaboration and Education***.** Herein lies the chief problem in dealing with Cyber Security in Africa; a lack of adequate knowledge of what to protect in cyberspace and how to deal with security incidences. He indicates that there is need for both Government, Private Sector and Academic institutions to have forums that discuss and tackle these cybersecurity challenges.

In the Private sector we have and see different challenges and threat actors. Sharing of solutions trends, intelligence and research is vital to keeping abreast in this dynamic field. These bodies lack the skills and technology needed to identify cybercrimes and perform forensic investigations that will lead to successful prosecutions of cybercrimes. On Education Musuva-Kigen e tal says that **there must be cybersecurity awareness for citizens in the use of internet, mobile banking and payment services; training of cyber security professionals and defenders, the Judiciary and Military; encouraging cyber security competitions and cyber clinics.**

He further notes that, **"academia forms the backbone of information security research. More academic institutions need to incorporate security awareness in their curriculum to promote further research on emerging cyber threats in Africa and develop innovation hubs for young talent in the area of cyber security.**"

(Chopra, 2014) also approves this by indicating that cybersecurity education must be embedded in the school curriculum starting from primary school level because once one better understands what cybercrimes are then cybersecurity measures can effectively be sought. **The only security tool in the cyber world is by learning hacking yourself** as security is just a feeling it does not exist in the actual world, or simply put if you want to make it more difficult to crack learn hacking yourself. (Chopra, 2014).

History is the witness that no legislation has succeeded in totally eliminating crime from the globe. "**The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world**.

On one hand, he does not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cybercrime and on the other, he cautions the pro-legislation school that it should keep in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive. He further indicates that, in other countries like India, police has initiated special cyber cells across the country specifically for cyber criminals and have started educating the personnel.

"Financial Services is a clear leader in this category (this is also true globally and within Africa) accounting for 86% of the total cybercrime incidents reported by Zambian respondents in 2016. The Communications industry has experienced a significant decrease in cybercrime over the last 24 months, while Government/State Owned Enterprises have experienced an increase in this type of crime whereas the sector previously reported zero incidents in 2014." (Thoithi, 2016 pp 18).The Communications industry and Government/State-Owned Enterprises in Africa also seem more vulnerable to this type of economic crime compared to other industries.

(Thoithi, 2016 pp 18), the results generated by his survey suggest that cyber-crime defense is still viewed as an "IT issue" as opposed to an organization-wide issue. **It is important for organizations to realize that the human or user aspect of an IT system is just at risk of breach (or even more) as the IT systems controls themselves. The implication is that any user of an IT system, whether they be IT personnel or a till manager at a point-of-sale terminal, could expose your organization to a cyber-crime threat.**

Indeed, social engineering[2] is a technique often used by perpetrators of cybercrimes. As such, it is not sufficient to view cybercrime as an IT issue. The entire organization must be on guard and prepared to deal with cybercrime threats. In his remarkable paper[3], Hathaway (2012), states that **a new, comprehensive legal framework at both the domestic and international levels is needed to more effectively address cyber-attacks.** Countries could strengthen their domestic laws by giving domestic criminal laws addressing cyber-attacks extra-territorial effect and by adopting limited, internationally permissible countermeasures to combat cyber-attacks that do not rise to the level of armed attacks or that do not take place during an ongoing armed conflict.

Yet the challenge cannot be met by domestic reforms alone. **International cooperation will be essential to a truly effective legal response**. New international

[2] Psychologically manipulating an individual into breaking security procedures or providing confidential information

[3] The Law of Cyber-Attack. Yale Law School Legal Scholarship Repository.

efforts to regulate cyber-attacks must begin with agreement on the problem—which means agreement on the definition of cyber-attack, cyber-crime, and cyber-warfare. This would form the foundation for greater international cooperation on information sharing, evidence collection, and criminal prosecution of cybercriminals.

Hathaway further insinuates that many countries including America have thus far largely failed to update legal frameworks that might respond to cyber- attacks. To face new and growing threats, governments continue to rely on limited and piecemeal bodies of law not designed to meet the challenge of cyber-attacks. It is past time to begin a conversation about the scope of the threat posed by cyber-attacks and the best ways to meet it. **Countries should expand the reach of domestic law abroad and develop a system for utilizing limited countermeasures where appropriate to respond to certain types of cyber-attacks.**

Until now individual countries are restricted in what they can accomplish alone. Cyber-attacks are often transnational—designed by authors in multiple countries, run through networks across the world, and used to undermine computer systems in countries where those designing the attack have never set foot. **This global threat may only be effectively met by a global solution—by the international community working together to design a new law for cyber-attacks.** He stresses that "cyber-attacks have become increasingly common in recent years. Capable of shutting down nuclear centrifuges, air defense systems, and electrical grids, cyber-attacks pose a serious threat to national security."

As a result, some have suggested that cyber-attacks should be treated as acts of war. For Dashora, **a nation with high incidence of crime cannot grow or develop that is so because crime is the direct opposite of development. It leaves a negative social and economic consequence.** In aggreeing with Doshora's assertion, Thoithi (2016 pp 18) in his elaborate research reveals that there are many associated risks with cybercrime and the increased rate of its occurrence has both a financial and non-financial impact on organizations.

Almost half of his respondents (49%) stated that their perception of the risks of cybercrime to their organization have increased since 2014 - and with good reason. Not only is the rate of cybercrime increasing worldwide but so is its impact. With regard to cybercrime, his respondents reported the highest impact to be financial loss. When asked to quantify those losses – the results showed that the quantum of financial losses had increased greatly from 2014 and the number of organizations reporting no loss from cybercrime dropped sharply (from 33% in 2014 to 9% in 2016).

Almost two thirds (65%) suffered a loss of below $100,000 compared to a much lower 19% indicated in his 2014 survey and the number of respondents suffering losses of between $100k-$1m also climbed from 7% in 2014 to 11% in 2016. A growing number of cybercrime incidents resulted in losses over $1 million (3% in 2016 from the 1% of 2014). These results are a cause for

concern and show that the threat of cybercrime is increasing in Zambia.

1.6 Establishment of the gap and Personal critique summary

Despite the many efforts made by countries in the quest of successful mitigation of cybercrime, the reviewed literature reveals numerous inadequacies in the required strategies in the fight against cybercrime in Zambia. In my analysis, I notice that there has not been discreet funding and sensitization to both the general populace and the stakeholders in the past. This was seemingly facilitated by the lack of government will power, inadequacies in cyber threats preventive infrastructure, ICT security policies and strong legal frameworks and, ICT human capital. To effectively mitigate the ever rising cases of cybercrime, institutions must seek to employ individuals with skills to defend against [4]crackers. Let institutions fund the cause of cybersecurity and partner with [5]certifying bodies to ensure that their cybersecurity employees are ever on pace with the dynamic trends in the cyber world. On all the literature provided, the modes of data collection and sampling were fine for they had near to zero negative influences on the data collected going by the presented information.

2. METHODOLOGY/RESEARCH DESIGN

2.1 Project Design / Approach

This chapter introduces the methods that were used in carrying out this study. These include the project design, sampling technique, target populations and sample size, instruments of data collection, data collection techniques, ethical considerations and data analysis. This was a hybrid research in that it incorporated both qualitative and quantitative research approaches and mainly employed desk research. Questionnaires were tailored in a way that was pertinent to the research demands. The internet as a source of data was heavily employed. Visitations to relevant institutions like the Ministry of Justice, Home Affairs Research and Information Development (HARID), National Anti-terrorism Center (NATC), Zambia Information and Communications Technology Authority (ZICTA), and Anti-Corruption Commission (ACC) were done and questionnaires were administered to the respective respondents and direct interviews with other special personnel were also conducted.

The research questions included but not limited to:

i. How does Zambia regard cybersecurity?
ii. How do Zambian Cyber Laws protect cybercrime victims in Zambia?
iii. What ways can be used to enhance the effectiveness of cybersecurity in Zambia?

2.2 Sampling procedure

To successfully gather the needed data, the researcher employed two main techniques. Purposive/judgmental and

[4] Black hat hackers/cybercriminals
[5] Like CISA, CNNA, CEH, CHFI…

Cluster. This was ideal seeing that in the former technique, the researcher chooses the sample based on who he/she thinks would be appropriate for the study. And the latter is mainly geographically driven. The main objective of purposive sampling is to arrive at a sample that can adequately answer the research objectives. The researcher would have a purposive sample accomplished by applying expert knowledge of the target population to select in a non-random manner a sample to represent a cross section of population. Wanjohi (2017).

2.3 Target populations and Sample size

The targeted study population was the Ministry of Justice, Home Affairs Research and Information Development (HARID), National Anti-terrorism Center (NATC), Anti-Corruption Commission (ACC) and Zambia Information and Communications Authority (ZICTA), all at their central offices. The afore mentioned institutions are charged with the authority to frame and explain laws, carryout assorted research pertinent to law and order, seek means of mitigating cybercrime, and regulate ICTs respectively. For that, they offered a wealth of information pertinent to the research topic in season ranging from explaining the cybersecurity context in Zambia, how cybercrime is handled in Zambia, who the main victims of cybercrime were and the detrimental effects of cybercrime.

2.4 Instruments of data collection

The mechanisms employed in data collection included the use of both questionnaires and interviews (See appendix II). The questionnaires were preferred in this study because those who took part in this study were considered to be literate and capable of answering the questions sufficiently. The researcher made personal visits to the respondents where a drop and pick later approach was employed. Interviews were conducted with the use of both structured and semi-structured modes of interview. Telephone interviews were also preferred to facilitate the research especially for areas where physical access to respondents was limited. The questions were structured in such a way that fixed response questions were rated against varying points scale form and room was provided for personal responses not captured in the fixed response-questions. The obtained responses were compared to the literature review to establish the significant implications of cybercrime on security.

The instruments of data collection used were self-constructed questionnaires designed in clear point like style to get the insight of the motivating factors of cybercrimes, victims and measures in Zambia to curb cybercrime. Awoniyi (2011), stated that a questionnaire is a self-reporting system of evaluation. It was widely used a tool owing to the fact that it is a flexible tool for data collection in research.

The researcher personally administered the hundred and five (105) self-constructed questionnaires to the respondents. These questionnaires covered many respondents at a time and short of them experiencing psychological anxiety.

ISSN: 3471-7102

2.5Data analysis techniques

The data from respondents was encoded and analyzed using descriptive statistics such as, percentages, tables and figures. Statistics/Data Analysis (STATA) was used to analyze the data.

2.6Ethical Considerations

To help in carrying out the research, the researcher sought for a letter of introduction from the Information Communication University Registrar's office, the Ministry of Justice, Home Affairs Research and Information Development (HARID), National Anti-terrorism Center (NATC), Anti-Corruption Commission (ACC) and Zambia Information and Communications Authority (ZICTA) before embarking on the research in the identified areas.[6]

3. RESULTS AND DISCUSSION

3.1. Results / Research findings

Data was collected from five (5) government institutions and fifty five (55) respondents drawn and the other fifty (50) private individuals with all of them responding. Cybersecurity simply denotes the technologies and procedures intended to safeguard computers, networks and data from unlawful admittance, weaknesses, and threats transferred through the internet by cyber delinquents.

The results in ***Table 1*** reveal interesting information concerning the cybersecurity context in Zambia and the ability of the Zambian cyber laws to protect cyber victims. It was noted that those with higher understanding as regards to cybercrime scored 11%, 41% for those with over-average understanding on the subject, 39% for those with lower understanding on the subject, 7% for those with near to zero information on the subject while 2% was for those not sure if they had information or not regarding cybercrime.

[6] Refer to Appendix

ISSN: 3471-7102

Table 1: Cybersecurity context in Zambia

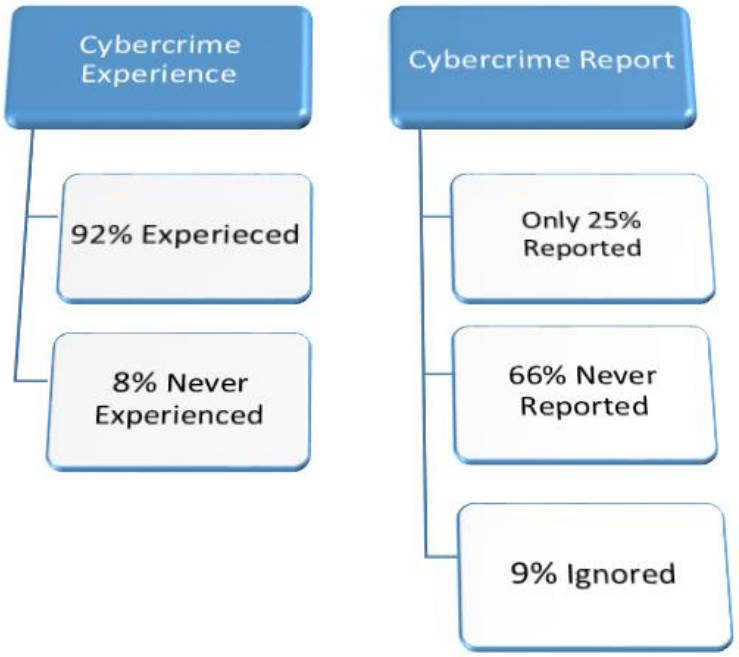
Comprehensive results			(%)
How often do you access internet?	1. Very often	57	57
	2. Often	31	31
	3. Rare	12	12
To what extent do you understand cybercrime/cyber-attacks?	1. Very high	11	11
	2. High	41	41
	3. Low	39	39
	4. Very low	7	7
	5. Not sure	2	2
Have you experienced any cyber-attack before? /heard someone experience it?	1. Yes	92	92
	2. No	8	8
If YES: Which one?	1. Loss of cash in bank account	42	42
	2. Loss of Airtime on mobile phone	6	6
	3. Hacked Facebook/E-mail	29	29
	4. Computer/Phone virus	0	0
	5. Leak of sensitive information	9	9
	6. Other (Specify) …	6	6
	7. Nil	8	8
How widespread are the cybercrimes/cyber-attacks in Zambia?	1. Very high	11	11
	2. High	41	41
	3. Low	39	39
	4. Very low	7	7
	5. Not sure	2	2
If 'YES' TO C9: How effective are the cybercrime Laws in Zambia?	1. Very effective	1	1
	2. Effective	33	33
	3. Not effective	40	40
	4. Not sure	8	8

Source: Research data

Cybercrime is simply a criminal activity that uses the internet and computers to commit a crime. 98 respondents from both stakeholders and private individuals consented to their knowledge and existence of cybercrime in Zambia (***Figure 1***). From the results in ***Table 1***, it was found that loss of cash from bank acount (through varied means such as [7]salami slicing), hacked facebook/email/phone and leaking of sensitive information and loss of airtime in mobile phones were the leading cybercrimes experienced by the respondents with 42%,39%,9% and 6% respectively.

[7] The action of taking tiny fractions of every transaction that builds into a large sum of illegally gained money www.computerhope.com/jargon/s/salami-slicing.htm

Most of these cases were not reported to relevant authorities to recover lost or damaged data. From ***Figure 1***, you will note that most victims prefered to keep quiet because they do not think reporting would help them since preserving of evidence is unknown to them. For financial institutions who were the main victims could not report in order to maintain credibility



Source: Research data

Notice that 92% experienced or atleast had heard about cybercrime save for the 8% who indicated their inexperience regarding cybercrime but only a miniature measure of 25% reported those cases to relevant authourities. 66% never reported while 9% opted to ignoring even after such an experience.

These statistics show that most Zambians and consumers of technology are initiating and falling victim of cybercrime, although the public are not reporting to relevant authorities either because of non-existent sensitization programs or hopelessness due to the unavailability of adequate cyber laws that would bring them justice.

ISSN: 3471-7102

Table 2: Effectiveness of the cyber laws in Zambia

How effective are cyber laws in Zambia?	Freq.	Percent	Cum.
Effective	33	33.00	33.00
Nil	8	8.00	41.00
Not effective	40	40.00	81.00
Not sure	18	18.00	99.00
Very effective	1	1.00	100.00
Total	100	100.00	

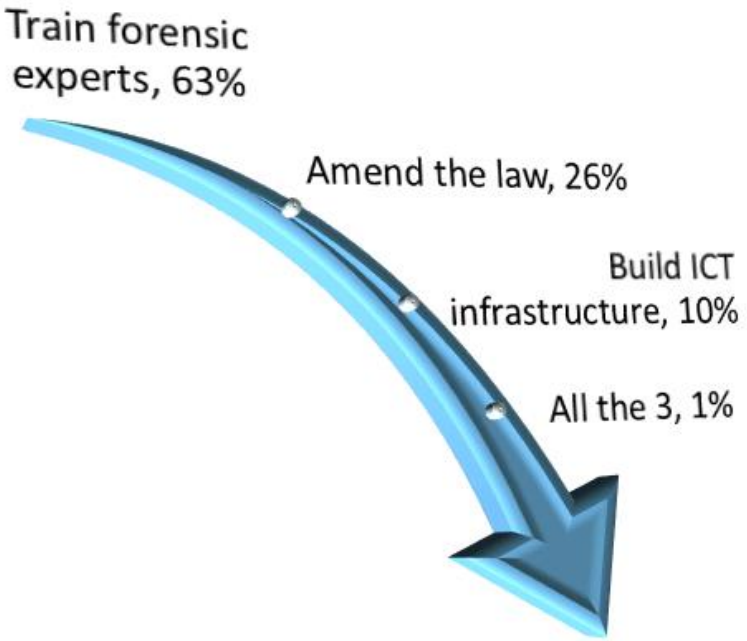
Source: Research data

On the other hand and instance, ***Table 2*** highlights the responses regarding the effectiveness of the cyber laws in Zambia as per the respondents' views. Where 1% for very effective, 33% effective, 40% not effective, 18% were not sure while the 8% represents those for a neutral ground.

Presently, the Zambian government is adopting a number of measures to establish client or user security and also ultimately reduce cybercrime. These measures vary and they are primarily instituted to control cybercrime from the public as much as possible who are largely not aware that this crime exists. The respondents were asked to identify the various measures needful in order to combat cybercrime. This was a four likert-scale where Train forensic experts=1, Amend the law=2, Build ICT infrastructure=3, and Other (specify) =4. The responses are in figure 2.

ISSN: 3471-7102

Figure 2: Measures to combat cybercrime



Source: Research data

The 50 respondents on the part of stakeholders and law enforcement were therefore queried on the type of IT certifications they owned. This was a four likert-scale where CCNA/CCNP/CCIE=1, CISA/CISM/CRISC=2, CHFI/CEH=3, Other (specify) =4, and None=5. Table 3 highlights their responses.

Table 3: IT Certifications

Certification owned	Freq.	Percent	Cum.
CCNA/CCNP/CCIE	5	10.00	10.00
CHFI/CEH	1	2.00	12.00
NCC	2	4.00	16.00
None	33	66.00	82.00
Other	9	18.00	100.00
Total	50	100.00	

Source: Research data

Table 3 reveals that by far the percentage (66%) most government departments had employed personnel not possessing rightful knowledge of cybercrime and protection of ICTs against cybercrimes. Notice that the certifications listed in Table 3 once acquired, one would have skills in auditing IT infrastructure and setting-up necessary controls to bar most threats to the network and computer systems. The information in Table 3 indicates that only 10% had

computer network(s) certifications, 2% had a qualifications in computer forensics/ethical hacking, 4%, 66% had no certifications of any form while 9% had other legal related certifications such as LLB.

Discussion

3.2. Discussion and Interpretation of Findings

In this section, the three core issues above are mapped with the research question results, to give the final and the most important findings in the research.

The first issue was to reveal the Zambian cybersecurity context. This relates to questions 2-5 of Table 1. Responses indicate that Zambia's regard to cybersecurity is weak.

The second issue was to find out how Zambian cyber laws protect victims of cybercrime in Zambia. This issue relates to questions 5 and 6 of Table 1. Responses indicate that cyber laws in Zambia are not effective enough to handle cybercrimes in their current state and are unable to adequately protect and save cybercrime victims.

The final issue concerns measures to be used to enhance cybersecurity in Zambia. This issue is mapped to Figure 2. The responses cited training forensic experts as the primary move with amendment of the law to be secondary, and tripled by building ICT infrastructure.

Presently, there is a lack of cybersecurity professionals in Zambia to protect the emerging ICT infrastructure and help identify system/network vulnerabilities that would lead into a portentous threats. There is therefore an urgent need of training cybersecurity professionals and defenders as other scholars like Musuva-Kigen e tal (2016 pp 52, 62) puts it.

Implications:

At present moment, private companies whose operations solely rely on the internet need to do more to protect themselves from cyber threats through training of their IT staff, capacity building and investment in IT security systems. Because the absence of cybersecurity experts means even with the presence of the much advocated-for legal frameworks there will be no compliance/risk-based auditing of information systems, investigation of cyber breaches and litigation of cyber delinquents.

CONCLUSIONS

In line with the general objectives of the study, the following conclusions were arived at:

The rise of technology has exposed organisations to a number of threats. There must be Cyber security awareness for citizens in use of internet, mobile banking and payment services; training of cyber security professionals and defenders, the Judiciary and Military; encouraging cyber security competitions and cyber clinics. To effectively do this, more academic institutions need to incorporate security awareness in their curriculum to promote further research on emerging cyber threats in Africa and develop innovation hubs for young talent in the area of cyber security.

It is important for organizations to realize that the human or user aspect of an IT system is just at risk of breach (or even

more) as the IT system controls themselves. This means that any user of an IT system, whether they be IT personnel or a till manager at a point-of-sale terminal, could expose your organization to a cyber-crime threat.

A new, comprehensive legal framework at both the domestic and international levels is needed to more effectively address cyber-attacks because this global threat may only be effectively met by a global solution—by the international community working together to design a new law for cyber-attacks this is essential to a truly effective legal response.

People must be made aware of their rights and duties (to report crime as a collective duty towards the society) and further make the application of the law more stringent in checking crime. A nation with high incidence of crime cannot grow or develop that is so because crime is the direct opposite of development. It leaves a negative social and economic consequence.

ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to Mr. Chuunga who served as my supervisor for his unwavering guidance and encouragement. I would also like to thank my friends for accepting nothing less than brilliance from me. Last but not the least, I would like to thank my parents and to my brothers and sisters for supporting me spiritually throughout writing this thesis and my life in general.

REFERENCES

[1]. Amazouz, S. (2016). *African Union Perspectives on Cybersecurity and Cybercrime*, Khartoum: s.n.

[2]. Awoniyi (2011). Introduction to Research. Sango, Ibadan: Ababa Press.

[3]. Awoniyi S.A. (2011). Introduction to Research lecture notes. Bulawayo: Zimbabwe.

[4]. Awoniyi S.A., Anderanti, R.A & Tayo, A.S (2011). Sango, Ibadan: Ababa Press.

[5]. Anderson, R. J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition, Wiley Publishing Inc., Indianapolis, Indiana

[6]. Chopra, S. (2014). *Why should we learn hacking?*. India: TEDxSIUHinjewadi..

[7]. Clarke, R. A. & Knake, R. (2010). "Cyber War: The Next Threat to National Security and What to Do About it," Ecco, (USA).

[8]. Dashora, K. (2011). *Cyber Crime in the Society*: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1, 240-259), pp. 1, 18.

[9]. Denning, P. J. & Denning, D. E. (2010). "Discussing Cyber Attack," Communications of the ACM, 53(9).

[10]. Eggers, W. D. (2016). *Government's cyber challenge: Protecting sensitive data for the public good.* [Online] Available at: https://dupress.deloitte.com/dup-us-

en/deloitte-review/issue-19/protecting-sensitive-data-government-cybersecurity.html [Accessed 25 may 2017].

[11]. Hathaway, O. A. (2012). *The Law of Cyber-Attack.* Yale: Faculty School series.

[12]. Infoguard AG. (2010). "Seminar on Ethical Hacking and Cyber Crime," Infoguard (Switzerland). available at [http://www.infoguard.com/ae/index.php?nav=108,126], [Retrieved June 3, 2011].

[13]. Jones, W. & Gallo, A. (2007). "A Process-Based Approach to handling Risks," IEEE – IT Professional, March/April 2007, 9(2).

[14]. Musuva-Kigen, P. (2016). *Africa Cyber Security Report*, Lavington, Kenya: Serianu Limited.

[15]. Rossi, B. (2016). *How to prevent the most dangerous cyber threat: insider attacks.* [Online] Available at: http://www.information-age.com/will-differential-privacy-take-favour-enterprise-123461324/ [Accessed 25 may 2017].

[16]. Lupiya S. (2009): *Cybercrime and the law in Zambia.* University of Zambia. Lusaka, Zambia.

[17]. Stead, C. (2016). *The true cost of cybercrime and why SME's are a target.* [Online] Available at: https://uk.smoothwall.com/true-cost-cybercrime-smes-target/ [Accessed 25 may 2017].

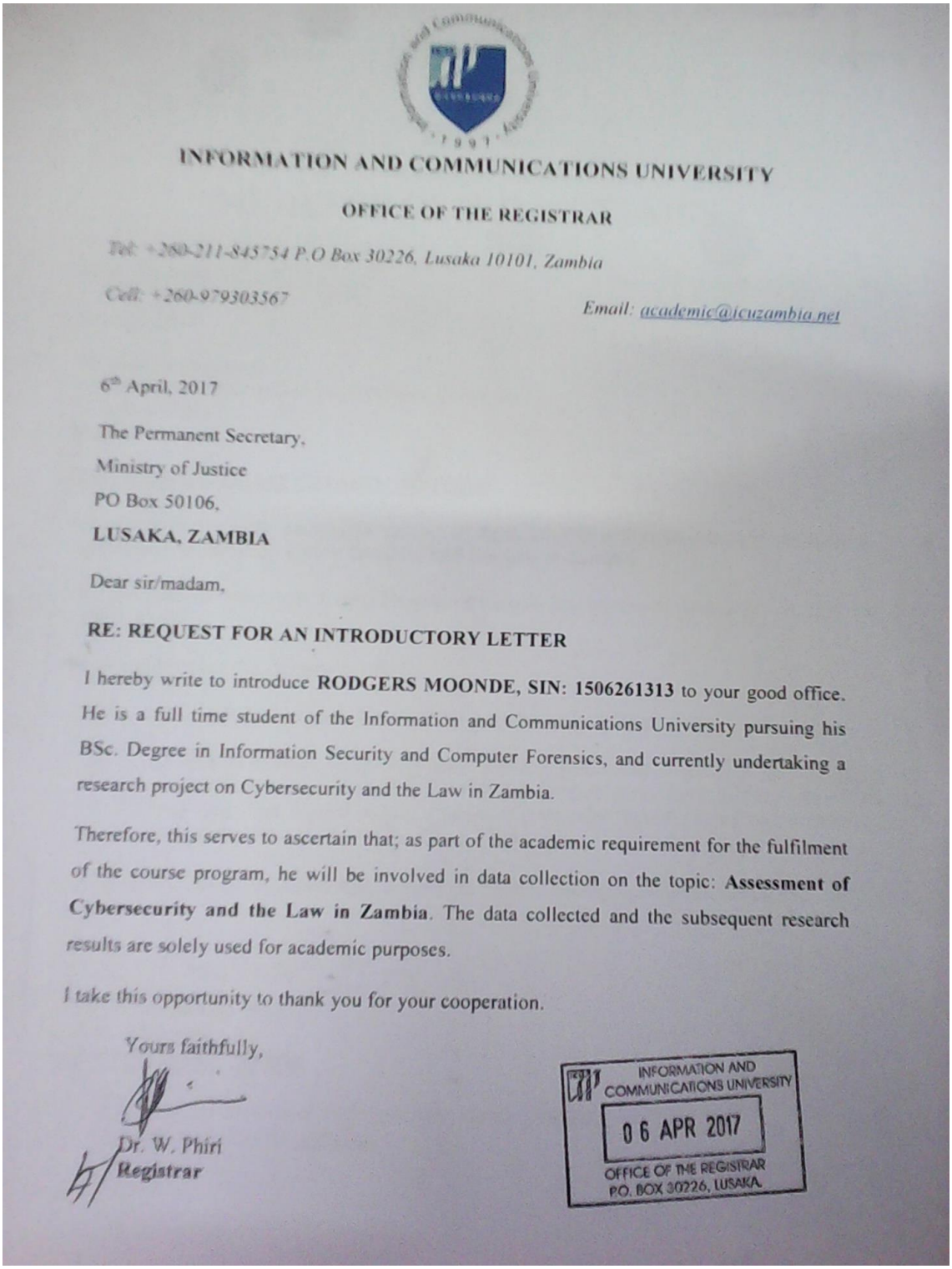
[18]. Savage, M. (2010). "Under Attack," Information Security, [Online], May 2010, [Retrieved June 3, 2011], available at: [http://viewer.media.bitpipe.com/1152629439_931/1272910610_295/0510_ISM_eM.pdf].

[19]. Thoithi, N. A. a. M. (2016). *Adjusting the Lens on Economic Crime in Zambia Turning opportunity for crime into opportunity for growth*, Lusaka: s.n.

[20]. Wanjohi M.A. (2017). *Sampling Procedures*: [Online] www.kenpro.org/samplingprocedures/. [Accessed 25 may 2017].

ISSN: 3471-7102

APPENDIX I: Permission for research



INFORMATION AND COMMUNICATIONS UNIVERSITY

OFFICE OF THE REGISTRAR

Tel: +260-211-845754 P.O Box 30226, Lusaka 10101, Zambia

Cell: +260-979303567 Email: academic@icuzambia.net

6th April, 2017

The Permanent Secretary,
Ministry of Justice
PO Box 50106,
LUSAKA, ZAMBIA

Dear sir/madam,

RE: REQUEST FOR AN INTRODUCTORY LETTER

I hereby write to introduce **RODGERS MOONDE, SIN: 1506261313** to your good office. He is a full time student of the Information and Communications University pursuing his BSc. Degree in Information Security and Computer Forensics, and currently undertaking a research project on Cybersecurity and the Law in Zambia.

Therefore, this serves to ascertain that; as part of the academic requirement for the fulfilment of the course program, he will be involved in data collection on the topic: **Assessment of Cybersecurity and the Law in Zambia**. The data collected and the subsequent research results are solely used for academic purposes.

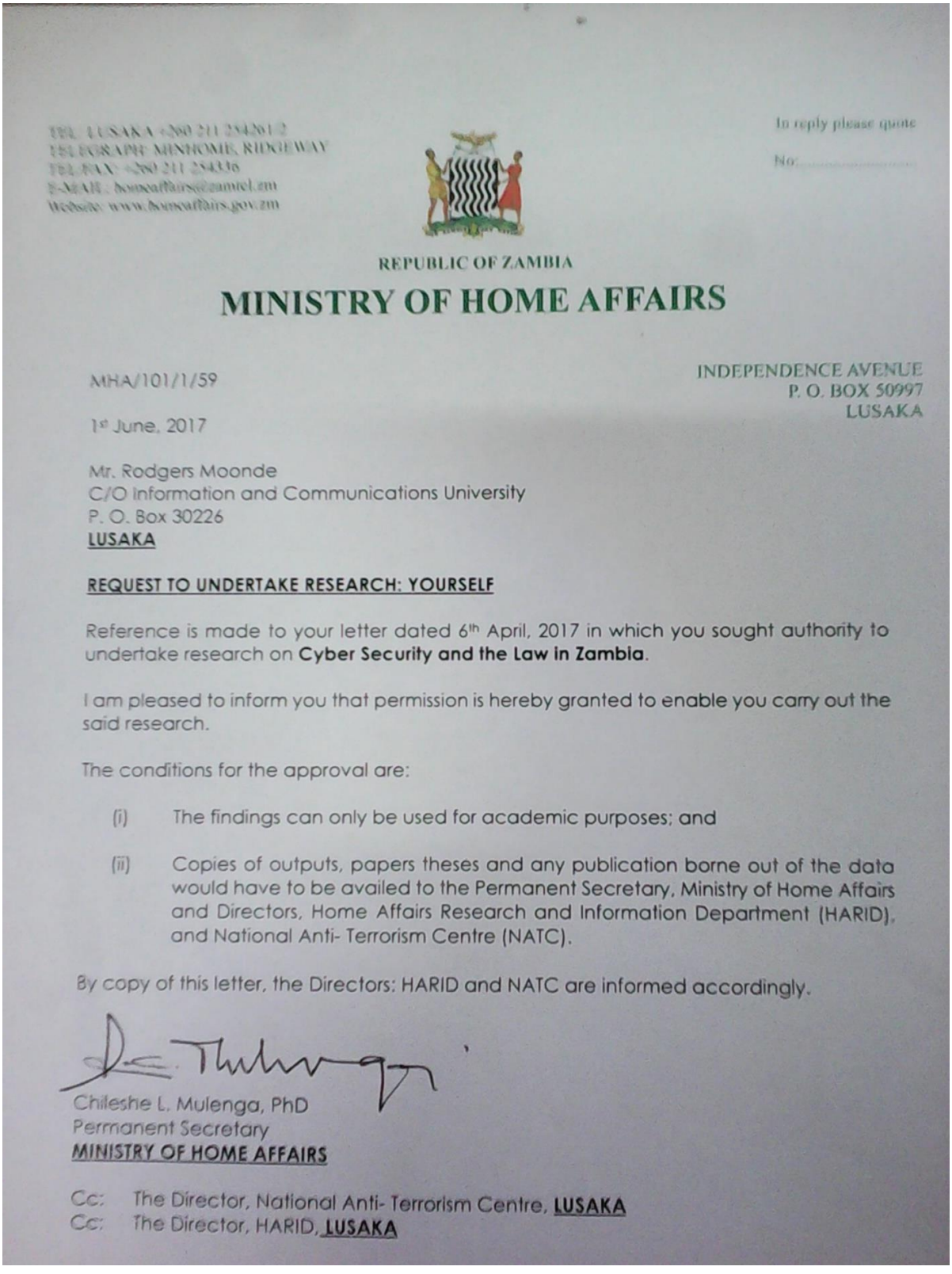
I take this opportunity to thank you for your cooperation.

Yours faithfully,

Dr. W. Phiri
Registrar

INFORMATION AND COMMUNICATIONS UNIVERSITY
06 APR 2017
OFFICE OF THE REGISTRAR
P.O. BOX 30226, LUSAKA

ISSN: 3471-7102



TEL: LUSAKA +260 211 254261/2
TELEGRAPH: MINHOME, RIDGEWAY
TEL/FAX: +260 211 254336
E-MAIL: homeaffairs@zamtel.zm
Website: www.homeaffairs.gov.zm

In reply please quote
No:.....

REPUBLIC OF ZAMBIA

MINISTRY OF HOME AFFAIRS

MHA/101/1/59

INDEPENDENCE AVENUE
P. O. BOX 50997
LUSAKA

1st June, 2017

Mr. Rodgers Moonde
C/O Information and Communications University
P. O. Box 30226
LUSAKA

REQUEST TO UNDERTAKE RESEARCH: YOURSELF

Reference is made to your letter dated 6th April, 2017 in which you sought authority to undertake research on **Cyber Security and the Law in Zambia**.

I am pleased to inform you that permission is hereby granted to enable you carry out the said research.

The conditions for the approval are:

(i) The findings can only be used for academic purposes; and

(ii) Copies of outputs, papers theses and any publication borne out of the data would have to be availed to the Permanent Secretary, Ministry of Home Affairs and Directors, Home Affairs Research and Information Department (HARID), and National Anti- Terrorism Centre (NATC).

By copy of this letter, the Directors: HARID and NATC are informed accordingly.

Chileshe L. Mulenga, PhD
Permanent Secretary
MINISTRY OF HOME AFFAIRS

Cc: The Director, National Anti- Terrorism Centre, LUSAKA
Cc: The Director, HARID, LUSAKA

APPENDIX II: Questionnaires

ISSN: 3471-7102

Name: _____

Job Title: _____

Do you think cyber security is a major problem in Zambia?

……

……

If yes, what do you think is the main cause of the Cyber security problem?

……

……

……

What can be done to improve the situational awareness in the country?

……

……

……

Do you think the private sector is investing enough in cyber security?

……

……

……

In your opinion, what drives criminals to commit cybercrime?

……

……

……

Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

……

……

Do you personally know of a company or individual who's been affected by cybercrime?

Were these cases reported to government authorities and prosecuted?

……

……

……

……

What do you think would be the best approach to address the cybercrime issue in Zambia?

……

……

……

……..

According to you, what is the most affected sector in the country regarding cybercrime?

……

……

……

From an African context, what would be the top

priority to address cybercrime across the continent?

……

……

……

The International Journal of Multi-Disciplinary Research

ISSN: 3471-7102

The 2017 International Multi-Disciplinary Conference on "Knowledge Sharing and Innovation Competitiveness for Responsive and Sustainable Development"

Research Issue

An Assessment of Cybersecurity and the Law in Zambia

Questionnaire ID

Dear respondent:

I **MOONDE RODGERS** a full-time student at the Information and Communications University and pursuing a Bachelor's Degree in Information Security and Computer Forensics is researching on the topic stated above.

You have been picked randomly via the use of probability techniques to participate in this research project. The purpose of this questionnaire is to gather sincere opinions about the subject. Your participation / contribution to this study will be highly appreciated. It is my sincere assurance that the findings generated from this study will be handled with the highest level of confidentiality and it is solely for academic reason and purpose. Be assured that all the information you will give, will be treated in utmost confidence and anonymity.

Please respond to the following questions as truthful as possible. Where there are options provided, select the appropriate response by putting a **NUMBER** of your choice in the provided box.

ISSN: 3471-7102

PART A: Demographic Data. *Fill in the boxes on Response with a **NUMBER** for your choice. Where writing is needed provide the appropriate response in the provided blank lines.*

Q. ID	Question	Response	For Official Use
A1	Province 1. Lusaka 2. Other (specify)……...		
A2	Gender 1. Male 2. Female		
A3	Age 1. 18-29 years 2. 30-40 years 3. Above 40 years		
A4	Professional Qualification 1. Certificate 2. Diploma 3. Degree 4. Masters 5. Other (specify) ……		
A5	Which profession better identifies you? 1. Lawyer/Judge 2. Software Engineer 3. Systems Engineer 4. Network Technologist 5. Forensic Scientist/Hacker 6. Other (Specify) ……..		
A6	Which of the fields below is associated to your qualification? 1. Business 2. Engineering 3. Lecturing 4. Legal 5. Security Other (specify)……		
A7	Which certification do you own? 1. CCNA/CCNP/CCIE 2. CISA/CISM/CRISC 3. CHFI/CEH 4. Other (specify) ……... 5. None		

A8	Employer 1. Private 2. Government		

PART B: Use of ICTs. *Fill in the boxes on Response with a **NUMBER** for your choice. Where writing is needed provide the appropriate response in the provided blank lines.*

Q. ID	Question	Response	For Official Use
B1	Do you own a computer (desktop/laptop/iPad)? 1. Yes 2. No		
B2	How would you rate your level of computer literacy? 1. Excellent 2. Good 3. Fair Poor		
B3	Do you own a mobile device and is able to access internet? 1. Yes 2. No		
B4	How often do you access internet? 1. Very often 2. Often 3. Rare 4. I do not		
B5	Where do you store your valuable data? 1. On internet 2. Memory Stick 3. Computer 4. Other (specify) ……..		
B6	Do you use licensed anti-virus software? 1. Yes 2. No		
B7	Have you got installed security cameras/CCTV? 1. Yes 2. No		
B8	Which of the following social media platforms are you mainly available? 1. Facebook 2. WhatsApp 3. Twitter 4. Other (specify) ……		

ISSN: 3471-7102

PART C: Cybersecurity and the Law. *Fill in the boxes on Response with a **NUMBER** for your choice. Where writing is needed provide the appropriate response in the provided blank lines.*

Q. ID	Question	Response	For Official Use
C1	Are you aware about cybercrime/cyberattacks? 1. Yes 2. No		
C2	If YES: how rampant are cybercrimes/ cyberattacks in Zambia? 1. Very high 2. High 3. Low 4. Very low 5. Not sure		
C3	Have you experienced/ (heard about) a cyberattack before? 1. Yes 2. No		
C4	If YES to C3: Which one? 1. Loss of cash in bank account 2. Loss of Airtime on mobile phone 3. Hacked Facebook/E-mail/Phone 4. Computer/Phone virus 5. Leak of sensitive information 6. Other (Specify) ……..		
C5	If YES to C3: Did you report the case to relevant authorities? 1. Yes 2. No		
C6	If YES to C5: Was it prosecuted? 1. Yes 2. No 3. Not sure		
C7	Does Zambia have Laws aimed at combating Cybercrime? 1. Yes 2. No 3. Not sure		
C8	If YES: How effective are the Cyber Laws in Zambia? 1. Very effective 2. Effective 3. Not effective 4. Not sure		
C9	If NO to C6: How do you handle cybercrime? 1. Ignore when it happens 2. Other (specify)……		

C10	Zambians do not care about Cybersecurity. To what extent do you agree to this assertion? 1. Strongly agree 2. Agree 3. Disagree 4. Strongly disagree		
C11	What measures must be placed to combat Cybercrime? 1. Train Forensic Experts 2. Build ICT infrastructure 3. Amend the Law 4. Other (specify)……	....	
C12	Cybercrimes are detrimental to National Economic Growth. To what extent do you agree to this assertion? 1. Strongly agree 2. Agree 3. Disagree 4. Strongly disagree		

…Thank you for your time….

The International Journal of Multi-Disciplinary Research

ISSN: 3471-7102

The 2017 International Multi-Disciplinary Conference on "Knowledge Sharing and Innovation Competitiveness for Responsive and Sustainable Development"

Research Issue

An Assessment of Cybersecurity and the Law in Zambia

Questionnaire ID

Dear respondent:

I **MOONDE RODGERS** a full-time student at the Information and Communications University and pursuing a Bachelor's Degree in Information Security and Computer Forensics is researching on the topic stated above.

You have been picked randomly via the use of probability techniques to participate in this research project. The purpose of this questionnaire is to gather sincere opinions about the subject. Your participation / contribution to this study will be highly appreciated. It is my sincere assurance that the findings generated from this study will be handled with the highest level of confidentiality and it is solely for academic reason and purpose. Be assured that all the information you will give, will be treated in utmost confidence and anonymity.

Please respond to the following questions as truthful as possible. Where there are options provided, select the appropriate response by putting a **NUMBER** of your choice in the provided box.

PART A: Demographic Data. *Fill in the boxes on Response with a **NUMBER** for your choice. Where writing is needed provide the appropriate response in the provided blank lines.*

Q. ID	Question	Response	For Official Use
A1	Province 3. Lusaka 4. Other (specify)……..		
A2	Gender 3. Male 4. Female		
A3	Age 4. 13-19 years 5. 20-35 years 6. Above 36 years		
A4	Level of education 6. Grade 7 7. Grade 9 8. Grade 12 9. College/University 10. None of the above		
A5	Employer 3. Private 4. Government 5. Self-employed 6. None of the above		

PART B: Use of ICTs. *Fill in the boxes on Response with a **NUMBER** for your choice. Where writing is needed provide the appropriate response in the provided blank lines.*

Q. ID	Question	Response	For Official Use

B1	Do you own a computer (desktop/laptop/iPad)? 3. Yes 4. No		
B2	How would you rate your level of computer literacy? 1. Excellent 2. Good 3. Fair 4. Poor		
B3	If POOR: are you willing to learn and become a leader of technology? 1. Yes 2. No		
B4	Do you own a mobile device and able to access internet? 3. Yes 4. No		
B5	How often do you access internet? 5. Very often 6. Often 7. Rare 8. I do not		
B6	Where do you store your valuable data? 5. On internet 6. Memory Stick 7. Computer 8. Other (specify) ……..		
B7	Which of the following social media platforms are you mainly available? 5. Facebook 6. WhatsApp 7. Twitter 8. Other (specify) ……		

PART C: Cybersecurity and the Law. *Fill in the boxes on Response with a **NUMBER** for your choice. Where writing is needed provide the appropriate response in the provided blank lines.*

Q. ID	Question	Response	For Official Use

C1	Do you own a Bank Account? 1. Yes 2. No		
C2	If NO: How do you keep your earnings? /what other way? 6. Use MTN/AIRTEL/ZAMTEL money services 7. Keep in-house 8. Other (specify)…….		
C3	To what extent do you understand cybercrime/cyberattacks? 1. Too high 2. High 3. Low 4. Too low		
C4	Have you experienced any cyberattack before? /heard someone experience it? 1. Yes 2. No		
C5	If YES: Which one? 7. Loss of cash in bank account 8. Loss of Airtime on mobile phone 9. Hacked Facebook/E-mail 10. Computer/Phone virus 11. Leak of sensitive information 12. Other (Specify) …….		
C6	If 'YES' to C5: Did you (they) report the case to relevant authorities? 3. Yes 4. No		
C7	If YES to C5: Was it prosecuted? 4. Yes 5. No 6. Not sure		
C8	How widespread are the cybercrimes/cyberattacks in Zambia? 1. Very wide 2. Wide 3. Not wide 4. Not sure		
C9	Does Zambia have Laws aimed at combating cybercrime? 4. Yes		

	5. No 6. Not sure		
C10	If 'YES' TO C9: How effective are the cybercrime Laws in Zambia? 5. Very effective 6. Effective 7. Not effective 8. Not sure		
C11	If 'NO' to C9: How do you handle cybercrime? 3. Ignore when it is experienced 4. Other (specify)……	…… …… ……	
C12	Zambians do not care about cybersecurity. To what extent do you agree to this assertion? 5. Strongly agree 6. Agree 7. Disagree 8. Strongly disagree		
C13	What measures must be placed to combat cybercrimes? 5. Train Forensic Experts 6. Build ICT infrastructure 7. Amend the Law 8. Other (specify)……	…… …… ……	
C14	Cybercrimes are detrimental to National Economic Growth. To what extent do you agree to this assertion? 5. Strongly agree 6. Agree 7. Disagree 8. Strongly disagree		

…Thank you for your time….