Maturity of cybersecurity initiatives in Malawi: A comparison with the drive for fast and ubiquitous Internet connectivity

Tiwonge Davis Manda, Malawi

Abstract

Africa, in general, and Malawi, in particular, have seen a significant increase in Internet-enabled infrastructure. Various efforts are also underway to significantly increase Internet connectivity speeds and access. The development of cybersecurity initiatives in Africa, however, is lacking. This study looks at the current state of cybersecurity initiatives in Malawi against a background of significant efforts to greatly enhance Internet connectivity speeds and access. Focus is therefore placed on cybersecurity-related standards, policies and legislation, and cybercrime law, as well as higher- and end-user-education programmes. The study concludes that despite registering remarkable progress in information and communication technology (ICT) infrastructure developments and related service roll-outs, Malawi is yet to make significant progress in the development of cybercrime legislation, higher-education programmes, end-user education, identity theft legislation, law enforcement for cybercrime, and standards and policies for cybersecurity.

Keywords: cybersecurity; cybercrime; legislation; education; Internet

Introduction

Africa is on the verge of a significant increase in Internet-enabled infrastructure, owing to the tremendous growth of wireless technologies and mobile Internet. Compared to this, however, the development of cybersecurity initiatives in Africa is lacking. For example, only a few countries have additional security measures apart from legislation (Cole *et al.*, 2008). In their study Cole *et al.*, (2008) found that Malawi had hardly any cybersecurity initiatives taking place at national level. For example, the country had no cybersecurity-related standards, policies, and legislation, or cybercrime law, as well as higher- and end-user-education programmes. A more recent study by the World Economic Forum found Malawi to be amongst the bottom 15 of 133 countries surveyed for ICT networked readiness (World Economic Forum, 2010).

It is obvious that in as much as the Internet has a lot of associated benefits, it also brings about significant security challenges. For example, the lack of adequate cybersecurity-related skills and the growing problem of spam are a drain on scarce and costly services, and are major concerns for developing countries (OECD, 2005). Over time, government entities and large corporations will increasingly be at risk of cybercrime. When communities become more dependent on the Internet, cybercrime becomes relatively easier to carry out (Cassim, 2009). In addition, there is a rise in sophisticated cases of cybercrime targeting some of the world's largest corporations and government entities (Security Watch, 2010).

This notwithstanding, the existence of appropriate legislation, experts, and educational programmes can play a significant role in enhancing cybersecurity. For example, education can play a significant role in fighting cybercrime through raising people's awareness of cybercrime and related risks, as well as highlighting the corresponding solutions (Awe, 2010). Untrained and apathetic users create an environment susceptible to damaging attacks on the information infrastructure (Cassim, 2009).

This paper investigates the current state of cybersecurity-related initiatives in Malawi, as well as contributing factors. It adopts a similar per-

This document has been produced by DiploFoundation with the financial assistance of the European Union. The contents of this document are the sole responsibility of the author and can under no circumstances be regarded as reflecting the position of the European Union or DiploFoundation.

spective to Cole *et al.*, (2008) and focuses on cybersecurity initiatives that relate to passive defence techniques. Focus is placed on cyber-security-related standards, policies, and legislation and cybercrime law, as well as on higher- and end-user-education programmes.

Research context

Malawi is located in southern Africa and is a member of the Southern African Development Community (SADC). The country covers a total land area of 94276 km^2, and has a population of about 13.1 million people. This represents a population density of 139 people/km^2 (NSO, 2008). The country's population is mostly rural based, with 84.7% of the population living in rural areas, where ICT-related infrastructure and service roll-out is generally poor. Despite this, Malawi has registered considerable growth in ICT-related service and infrastructure development over the past decade, especially around mobile cellar telephony. For example, between the years 2000 and 2009, the number of mobile telephony subscribers jumped from 0.41% to 15.7% of the population. Figure 1 shows trends in fixed-line telephony and mobile cellular subscriptions, and estimated Internet use.

Parallel to the remarkable investments in mobile cellular telephony, Malawi has also recently registered considerable efforts around mobile banking (mBanking) and broadband Internet service and infrastructure development. For example, the country's main fixed line telephony operator – Malawi Telecommunications Limited – has invested around $55 million in rolling out a fibre network cable both within the country and to the rest of the world through the Eassy and Seacom undersea cables (Chimwala, 2009). The Malawi Electricity Supply Commission is also undertaking a similar initiative, deploying a fibre network cable to connect major cities and higher education and research institutions.

Literature review

Any element of cyberspace can be at risk, despite having varying potential of the significance of risks they may attract (Fischer, 2005). According to Fischer (2005), cyber-security comprises the following three aspects:

1. Measures to protect information technology; the information it contains, processes, and transmits, and associated physical and virtual elements (which together comprise cyberspace).
2. The degree of protection resulting from application of those measures.
3. The associated field of professional endeavour.

Cybercrime

Cybercrime is defined as 'any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime,

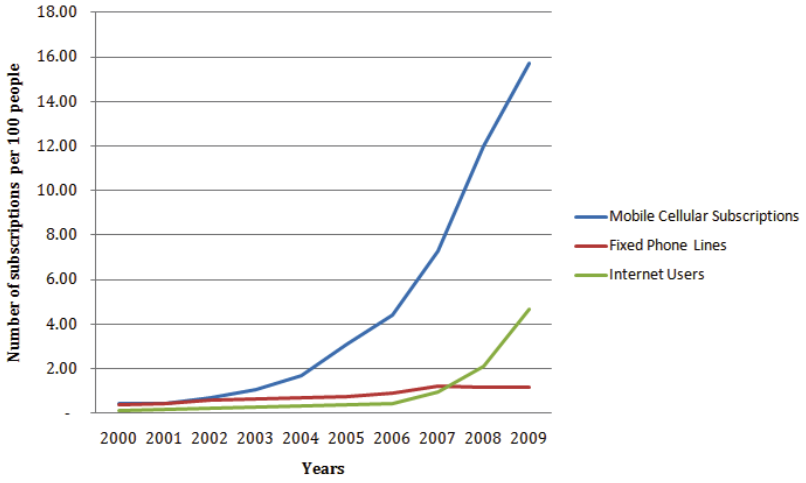

Figure 1. Trends in fixed-line and mobile cellular subscriptions and Internet use (ITU, 2011).

or the target of the crime' (Fossi *et al.*, 2008). It has been noted that despite registering positive strides in ICT, sub-Saharan Africa has also witnessed a surge in the use of these technologies for criminal activities and other social ills (Longe *et al.*, 2009). With current and persistent changes in technology, cyber-attackers keep enhancing the sophistication of their attack strategies and techniques (Grobler and van Vuuren, 2010). Observed crimes include identity theft, e-mail scams, trafficking, sexual exploitation, and prostitution (Longe *et al.*, 2009). In addition, the growing problem of spam has also been noted as a drain on scarce and costly services for developing countries (OECD, 2005). Such problems are likely to persist; there has been a global rise in sophisticated cases of cybercrime targeting some of the world's largest corporations and government entities (Security Watch, 2010).

Cybercrime legislation

Having the right laws in place is important: 'for an action to constitute a crime it must be prohibited by law, and a punishment must be prescribed for such action' (DiploFoundation, 2010). The upsurge in cybercrime can partly be attributed to severe shortcomings of both local and international legislation (Grobler and van Vuuren, 2010). Traditional law enforcement tools are quite lacking in dealing with cybercrime (Cassim, 2009). This is because technologically mediated crimes differ in the methods used in their commission, as well as in the nature and extent of the resulting harm (Brenner, 2004). This, therefore, calls for the development of new metrics and legislation to deal with cybercrime (Brenner, 2004; Cassim, 2009).

Capacity development

African states need to invest in human capacity development if they are to realise the desired economic growth from current investments in information infrastructure (Holmner *et al.*, 2010). Investing in cybersecurity-related higher- and end-user-education programmes is one way of doing this. Higher-education cybersecurity programmes are critical for the creation of technical jobs, as well as the development of a workforce that can contribute towards alleviating a nation's security concerns. On the other hand, cybersecurity education for end-users is necessary to help individuals safeguard their private information (Cole, Marshini Chetty *et al.*, 2008). Education raises people's awareness of cybercrime and related risks, as well as the corresponding solutions (Awe, 2010). On the contrary, untrained and apathetic users create an environment susceptible to damaging attacks on the information infrastructure (Cassim, 2009).

Methodology

This study adopted a qualitative case study approach as the methodology allows for intense investigation of a system or a phenomenon in its real-life context (Lee *et al.*, 2010). Furthermore, case studies allow the researcher to describe, explore, and explain a particular system or phenomenon in depth (Lee *et al.*, 2010). Data for the research was collected through a blend of primary and secondary sources: a combination of semi-structured interviews, a qualitative review of literature, and document analyses. Key informants interviewed include the Director of ICT and E-Learning at Chancellor College, the Head of the Department of Computing and Information Technology, at the Malawi Polytechnic. Chancellor College and the Malawi Polytechnic are constutuent colleges of the University of Malawi. The Malawi Government Wide Area Network (GWAN) Manager was another key informant in the study. Two lawyers, one from Chancellor College and another from the State Advocate Chambers, were also consulted for information on existing legal instruments on cybercrime.

Qualitative interviews were chosen because they allow the researcher to go below the surface of the topic being discussed and explore what people say in more detail. Furthermore, interviews allow the researcher to seek immediate clarification from the respondent when needed (Britten, 1995). On the other hand, a qualitative review of literature and document analyses enabled this study to triangulate various findings, as well as relate cybersecurity initiatives in Malawi with those from across the globe. Key documents from Malawi that were consulted

include: the 1998 Communications Act; ICT policy; ICT4D policy; current and proposed ICT curricula from two constituent colleges of the University of Malawi – Chancellor College and the Malawi Polytechnic; ICT curricula from Mzuzu University and DMI-St John the Baptist University; and draft cybersecurity bills.

Further to this, the study considered a downsized list of initiatives from that used by Cole *et al.*, (2008) in a previous study on cybersecurity initiatives in Africa, in which initiatives from Malawi were also reviewed. This study investigated cybersecurity initiatives from Malawi around the following dimensions: cybercrime legislation, higher education programmes, end-user education, identity theft legislation, law enforcement for cybercrime, and standards and policies for system security measures.

Findings

ICT initiatives

As already indicated, over the past few years Malawi has registered remarkable progress in ICT infrastructure development and related service roll-outs. For example, the country's main fixed line telephony operator – Malawi Telecommunications Limited – has invested over $55 million in rolling out a fibre network cable (Chimwala, 2009). The Malawi Electricity Supply Commission (ESCOM) is also undertaking a similar initiative, deploying a fibre network cable to connect major cities and higher education and research institutions. The country's two mobile telephony operators have also rolled out 3G cellular telephony services. At the moment, these services are targeting major cities and resort areas. In addition to these efforts, several banks have also rolled out mBanking services. From February 2011, salaries for Malawi's civil servants are only being paid through bank accounts. This, then, necessitates the roll-out of better ICT-related services like mBanking and e-payment systems to under-banked, rural areas. This would permit civil servants better access to their money. The country's draft ICT and ICT4D policies call for such initiatives and more. For example, the country's ICT4D policy advocates the need for universal access to Internet connectivity. A majority of the country's population lives in rural areas where access to ICT services and infrastructure is poor.

Cybersecurity and cybercrime initiatives

Currently, Malawi has no cybercrime legislation and law enforcement measures for cybercrime. The country also has no known standards and policies for system security measures. However, the country is currently in the process of developing an amendment to the Communications Act, which, among other things, introduces more focus on information society issues. Malawi's current Communication Act of 1998 predominantly focuses on regulating postal and broadcast services.

The country is also in the process of developing various e-legislation instruments with a focus on data privacy, digital signature management, as well as other aspects of cybersecurity. These efforts, though, are at an early stage, with the country's Department of Information Systems and Technology Management Services currently trying to engage a consultant to help with their development. The department aims to have the target e-legislation instruments ready for presentation to cabinet and debate in parliament towards the end of 2011.

Prior to these current efforts, a draft bill on e-signature management was developed in 2003. However, due to various factors, the effort did not materialise and the bill was never tabled for debate in parliament, and possible passing into law.

Capacity development initiatives

This study did not find any ongoing end-user training programmes on cybersecurity. Focus is therefore paid to higher-education programmes on cybersecurity. In line with this, curricula for several institutions providing higher education were looked at. Table 1 presents a summary of cybersecurity-related content offering at various higher-education institutions.

It should be noted that although the DMI-St John the Baptist University has a programme in Computer Security at undergraduate level, the university has just opened its doors in Malawi and is in the process of enrolling its first intake of students. The first crop of computer security professionals trained within Malawi is therefore likely to graduate in four years' time.

Reasons for the current state of initiatives in Malawi

Reasons for the weak drive in cybersecurity-related initiatives are varied. First, there is a lack of adequate trained personnel with advanced knowledge of cybersecurity. It is not easy for such multistakeholder initiatives to move forward when there are not enough people who can ably participate. Secondly, cybercrime in Malawi is yet to significantly pick up or register devastating consequences. Some respondents indicated that Internet connectivity is currently slow, which makes exploitation of networked systems both slow and difficult. The respondents indicated that because of this, end-users do not see a great need for extra measures to protect their data, besides safeguarding it against viruses.

In addition to these factors, one key respondent indicated that working culture does play a role, as even after the realisation of the importance of undertaking certain ICT initiatives, movement is generally slow. An example is the Malawi ICT policy, which is still in draft form over 10 years after its development process was first initiated.

With regard to the failed initiative in 2003 to have in place a Digital Signature Management Act, change in government policy was noted as one of the reasons for the failure. The development of the Act was tied to a proposed establishment of a directorate to manage ICT. The government was at the time moving away from introducing new directorates and this negatively impacted this effort.

There are also indications that ICT professionals, possibly through the ICT Association of Malawi, have not been proactive enough to try and create awareness of a potential upsurge in cybercrime and the corresponding need for appropriate cybercrime legislation and cybersecurity initiatives, once Internet connectivity becomes fast and ubiquitous.

Discussion

As the findings indicate, Malawi still has a long way to go as regards the development of the necessary legal frameworks, standards, and capacity to enhance cybersecurity and keep cybercrime in check. The many emerging fronts for ICT development and the slow pace in pushing cybersecurity initiatives stand to pose considerable cybercrime risks as Internet connectivity becomes fast and ubiquitous. With current and persistent changes in technology, cyberattackers keep enhancing the sophistication of their strategies and techniques (Grobler and van Vuuren, 2010). The Malawi government's efforts outlined in the country's ICT and ICT4D policy to achieve universal Internet access, as well

Table 1. *A summary of Information Security modules at tertiary level in Malawi.*

Institution	Full degree programmes	Modules currently being offered - Undergraduate	Proposed modules - Undergraduate
Chancellor College	None	None	• Computer Security • IT Audit and Controls • E-Business Techniques
The Malawi Polytechnic	None	Computer Security and Firewalls	Information Systems Audit
Mzuzu University	Master of Science programme in Information Theory, Coding and Cryptography	Network administration and Information Security	
National College of Information Technology	None	Internet Security and Management	
DMI-ST John the Baptist University	• Bachelor of Science in Computer Security		

as having in place relevant legal frameworks to promote ICT use cannot be effectively realised within the current set-up. Malawi is walking the same line as other sub-Saharan African countries who, according to Longe *et al.*, (2009), have witnessed a surge in ICT-driven criminal activities and social ills, resulting from positive developments in ICT. That appropriate legal frameworks are needed to fight such imbalances needs no further emphasis. Technologically mediated crimes differ in the methods used in their commission, as well as in the nature and extent of the resulting harm (Brenner, 2004). This, therefore, calls for the development of new metrics and legislation to deal with cybercrime (Brenner, 2004; Cassim, 2009).

On the other hand, in as much as cybersecurity initiatives in Malawi are still at an early stage, in the drive for fast and ubiquitous Internet connectivity, the country has registered some positive movement since 2008 when a study by Cole *et al.*, (2008) established that there were hardly any cybersecurity initiatives in the country at all.

Cybersecurity-related capacity development

It has been noted that African states need to invest in human capacity development if they are to realise the desired economic growth from current investments in information infrastructure (Holmner *et al.*, 2010). Higher-education cybersecurity programmes, for example, are critical for the creation of technical jobs, as well as the development of a workforce that can contribute to alleviating a nation's security concerns. On the other hand, cybersecurity education for end-users is necessary to help individuals safeguard their private information (Cole *et al.*, 2008). Education raises people's awareness of cybercrime and related risks, as well as corresponding solutions (Awe, 2010). On the contrary, untrained and apathetic users create an environment susceptible to damaging attacks on the information infrastructure (Cassim, 2009). In as much as this is the case, the development of cybesecurity-related competencies for both professionals and end-users in Malawi will most likely take time before noticeable changes can be registered. For example, despite the DMI-St John the Baptist University offering a Bachelor of Science in Computer Security, the university's first intake of students will graduate around the year 2014. On the positive side, Mzuzu University's Master of Science programme in Information Theory, Coding, and Cryptography has been running for some years and is well established. Besides these two universities, other higher education institutions will, for some time, be limited in their cybersecurity-related course offers due to a lack of adequate personnel with relevant expertise. Even when expertise is available, both technology and threats will have evolved, making it hard for user training and education to keep in step (Fischer, 2005).

Need for cultural change

Looking at the historically slow pace with which other ICT initiatives like the Malawi ICT policy have been developed, it remains to be seen whether the country will be able to develop a timely regulatory and legal framework that promotes more secure ICT use. For the current initiatives to succeed there is not only a need for technocrats who can direct such initiatives, but also for changes in working culture.

Culture impacts innovation by shaping how people respond to new things and how they collaborate, as well as how people understand risks and opportunities and, in turn, respond to these, too (Beardsell, 2009). Although culture is changeable, it must be noted that culture is influenced by multiple factors; large-scale cultural change is usually a slow process (Pollard *et al.*, 2010). This should be even more in the case of multistakeholder initiatives like the development of necessary cybersecurity-related standards, legal frameworks, and competencies. In as much as multistakeholder platforms seek to enable empowered and active participation of stakeholders, challenges do exist. For example, such initiatives need to deal with issues relating to power relationships, choice of the composition of the multistakeholder initiative, and stakeholder representation and capacity to ably participate in debates, and decision-making of such platforms (Faysse, 2006).

Conclusion

Despite registering remarkable progress in ICT infrastructure developments and related service roll-outs, Malawi is yet to make significant progress in the development of cybercrime legislation, higher-education programmes, end-user education, identity theft legislation, law enforcement for cybercrime, and standards and policies for cybersecurity. Although there is some positive movement around these initiatives, it is unclear as to when necessary standards and legal frameworks, as well as competencies, will be significantly developed to check cybercrime and promote more appropriate use of ICT. At the moment, there is not much drive on these initiatives compared to the drive and buzz around fast and ubiquitous Internet connectivity.

Reasons for the current state of events range from lack of adequate technical capacity to drive the development of cybersecurity-related instruments and educational programmes, a working culture of not promptly responding to ICT-related changes, as well as a current absence of significant cybercrime.

Considering the current upsurge in ICT infrastructure development as service roll-outs, such as 3G Internet services and mBanking, and the drive for universal access to relevant ICTs, it is imperative that Malawi moves quickly in developing cybercrime legislation, higher-education programmes, end-user education, identity theft legislation, law enforcement for cybercrime, and standards and policies for cybersecurity. This will help safeguard critical information and infrastructure, as well as maintain user trust in ICT initiatives over the long term. User trust is critical to continued and sustainable ICT development.

References

1. Beardsell J (2009) Managing Culture as Critical Success Factor in Outsourcing. SMC Working Paper Series 9.
2. Brenner S W (2004) Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology* 9(4).
3. Britten N (1995) Qualitative Research: Qualitative interviews in medical research. *BMJ* 311: 251– 253.
4. Cassim F (2009) Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comperative Study. *PER* 12(4): 36-79.
5. Chimwala M (2009) Malawi sets aside $55m for fibre-optic network. Available at http://www.engineeringnews.co.za/article/malawi-telecoms-2009-07-31 [Accessed 13 March 2011].
6. Cole K *et al.*, (2008) *Cybersecurity in Africa: An Assessment*. Atlanta,Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.
7. Diplo Foundation (2010) *Introduction to Policy Research. Security Research I*, Diplo Foundation.
8. Lee E *et al.*, (2010) How to Critically Evaluate Case Studies in Social Work. *Research on Social Work Practice* 20(6): 682-689.
9. Faysse N (2006) Troubles on the way: An analysis of the challenges faced by multi-stakeholder platforms. *Natural Resources Forum* 30(3): 219-229.
10. Fischer E A (2005) *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, Congressional Research Service*. The Library of Congress.
11. Fossi M E *et al.*, (2008) Symantec Report on the Underground Economy, Symantec.
12. Grobler M and van Vuuren J J (2010) Broadband Broadens Scope for Cyber Crime in Africa. *Proceedings of the 2010 Information Security for South Africa:* pp 1-8.
13. Holmner M *et al.*, (2010) The last mile or the lost mile? The information and knowledge society in Africa. *Proceedings of SIG GlobDev Third Annual Workshop*, Saint Louis, USA.
14. ITU (2011) World Telecommunication/ICT Indicators Database: Key 2000-2009 Country Data International Telecommunications Union.
15. Longe O *et al.*, (2009) Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact* 9(3): 155-172.
16. NSO (2008) 2008 *Population and Housing Census Main Report*. Zomba, National Statistical Office.
17. OECD (2005) *Spam issues in developing countries*. Paris, Organisation for Economic Cooperation and Development (OECD).
18. Pollard M P J *et al.*, (2010) Why Information Technology (IT) Systems – led Organisational Change Does not Work. *International Journal of Business, Management and Social Science* 1(1): 88-99.
19. Security Watch (2010) Cybercrime grows despite economic slowdown. Available at http://www.securitywatch.co.uk/2010/04/20/cybercrime-grows-despite-economic-slowdown/ [Accessed 14 May 2010].
20. World Economic Forum (2010) The Global Information Technology Report 2009–2010. Available at http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm [Accessed 7 March 2011].