IBIMA Publishing
Journal of Information Assurance & Cybersecurity
http://www.ibimapublishing.com/journals/JIACS/jiacs.html
Vol. 2012 (2012), Article ID 322399, 10 pages
DOI: 10.5171/2012.322399

Research Article

A Framework for Cyber Security in Africa

E Kritzinger[1] and SH von Solms[2]

[1]University of South Africa, Pretoria, South Africa

[2]University of Johannesburg, Johannesburg, South Africa

Received 4 August 2012; Accepted 8 October 2012; Published 30 December 2012

Academic Editor: Dhayalan Velauthapillai

Abstract

This paper deals with at least four major cyber safety concerns in Africa discussed in recent literature. These cyber concerns include aspects such as policies, procedure, awareness, research and the provision of technical security measures. Each concern is examined, the main focus areas are highlighted and a solution is proposed. This paper concludes by combining all relevant solutions into a proposed cyber security framework to assist Africa in decreasing its cybercrime rate especially among home users with no or limited cyber safety knowledge.

Keywords: Cyber security, Africa, information service providers, awareness.

Introduction

The latest figures show the increase of cyber users all over the world. This has in a sense inadvertently opened the door to an increase in cyber crimes and threats associated with being connected especially in Africa (Cole et al., 2008). Akuta, Ong'oa and Jones put it unashamedly when they say that "Literature indicates that, out of the top ten countries in the world with high levels of cybercrime prevalence, sub-Sahara Africa is host to four of these countries (Nigeria, Cameroon, Ghana and South Africa)" (Akuta, Ong'oa and Jones, 2011). The main reason forwarded for the increase of cybercrime particularly in Africa is the sudden increase in the use of information communication technologies (ICTs) in a number of African countries. Akuta et al. are spot on when they argue that "With a new decade beginning, the continent of Africa, which was regarded as 'backwards' has been able to get a leap into the work of ICT" (Akuta, Ong'oa and Jones, 2011). This rapid leap of using ICTs and broadband opens a gap for a number of cyber threats that can result in cybercrime.

Rowe, Reeves, Wood and Braun are very concerned with the threats that seem to be engulfing the African continent. They voice their concern in this way, "The worrying news for cyber security experts is that broadband services are opening in the continent, which means more users would be able to access the web, translating into more viruses and spam from online" (Rowe, Reeves, Wood and Braun, 2010). The worse part of it all perhaps is that many of these users, sadly, do not have a clue as to how to protect themselves and their personal information against the cyber attacks directed at their gadgets.

Rowe et al. paint a frightening picture about the level of cyber security threats in the African continent as a whole. They argue that "about 80 percent of PCs in the African continent are already infected with viruses and other malicious software" (Rowe, Reeves, Wood and Braun, 2010). While this

Copyright © 2012 E Kritzinger and SH von Solms. This is an open access article distributed under the Creative Commons Attribution License unported 3.0, which permits unrestricted use, distribution, and reproduction in any medium, provided that original work is properly cited. Contact author: E Kritzinger E-mail: kritze@unisa.ac.za picture alone is very threatening, it is further alarming to note that it is not only personal computers (PCs) that are affected in Africa as a whole. Cybercrime is slowly starting to exploit mobile devices in Africa too. Greenwood knows exactly where this problem emanates from when he reports that, "in the rapidly evolving mobile landscape in Africa, the growth has been fuelled in large part by the liberalization effort resulting in the formation of independent regulatory bodies and increased competition in the market. The total African mobile subscriber base is roughly 280.7 million people (30% of the total); with at least 15 mobile operators already having announced plans of introducing 3G and data services (including Tanzania, Kenya and Nigeria)"(Greenwood, 2009).

This increase in mobile use (mobile phones with web connectivity) is opening the door for all cyber criminals to exploit mobile users with little or no cyber safety knowledge. "More individuals worldwide gain Internet access through mobile phones. Cyber criminals will have millions of inexperienced users to dupe with unsophisticated or well-worn scamming techniques that more savvy users grew wise to (or fell victim to) ages ago" (Ciso, 2009).

In many of these cases, laypeople are not aware of the cyber danger surrounding them. They are just happy that they can operate their gadgets and it would seem not enough is done to train and educate them in using these safely. Jensen confirms these fears when he states that, "the availability of specialist training in telecommunications is currently extremely limited on the continent [Africa]" (Jensen, 2001).

The main focus of this paper is to attempt to address cybercrime within Africa. This paper starts by investigating different cyber security problems in Africa and highlights four major cyber concerns currently connected to Africa. It primarily investigates these four concerns and proposes possible solutions for each. The paper concludes by combining all the solutions into a proposed cyber protection model that incorporates different cyber viewpoints in an attempt to decrease cybercrime in Africa.

Some Major Cyber Security Problems in Africa

Four different types of cyber problems are mentioned in this section in an attempt to address the worrying question of cybercrime in Africa. These cyber problem areas overlap to some extent; however, each problem is individually addressed.

Problem 1: Lack of Focused Research in Cyber Security

A number of cyber factors have led Africa to becoming a cybercrime hub. According to Von Solms and Kritzinger, these factors include the following (Von Solms and Kritzinger, 2010):

- Increasing bandwidth,
- Increasing use of wireless technologies and infrastructure,
- Lack of cyber security awareness,
- Ineffective legislation and policies,
- Lack of technical cyber security measures

Because many, if not all, of these cyber problems facing the African continent are, to a certain extent, unique to Africa and other developing countries, solutions imported directly from developed countries do not always work wonders in Africa. Focused research in Africa for Africa is required to create new cyber security solution for the continent.

Jensen believes that "African countries can make leapfrog jumps forward in communication connectedness by adopting new technologies – necessarily using different strategies than developed countries followed" (Jensen, 2001).

Problem 2: Lack of a Proper Integrated Framework on Legal and Policy Aspects

The problem in cybercrime in the African continent identifies loopholes that exist among different stakeholders in the war against cybercrime. Akuta et al. believe that we need proper and relevant laws, policies and practices if we are to fight cybercrime successfully in this continent (Akuta, Ong'oa and Jones, 2011). This is war and we need to use every arsenal in our reach to deal with it decisively. Rowe et al., for example, correctly state that "most African countries have no legal regulations in place to stop or prosecute online crime, thus providing a safe haven for cyber criminals" (Rowe, Reeves, Wood and Braun, 2010).

Problem 3: Lack of Cyber Security Awareness and Regulation

The third problem investigates a different view of cybercrime. This problem addresses mainly the aspects regarding cyber awareness and regulation. Kritzinger and Von Solms are mainly concerned about the awareness created or lack of it about cybercrime (Kritzinger and Von Solms, 2010). In this regard, Kritzinger and Von Solms are supported by Kumar who plainly state that "almost 80 percent of the population in Africa lacks even basic knowledge of computers. Internet cafés, though widespread, are unable to afford antivirus software, making them easy targets for hackers and botnet operators" (Kumar, 2010). This is a very risky situation and means therefore that there is a clear, but certainly not deliberate lack of cyber security awareness and education to make cyber users aware of all possible cyber threats and risks.

Problem 4: Lack of Technical Security Measure

The last problem focuses on the technical aspects of cyber safety. Cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched. A solution is needed to ensure that such computers are technically secured by taking the responsibility away from the user and giving it to a third party.

Proposed Cyber Security Solutions

This section will revisit the four current cyber security problems in Africa and propose a possible cyber solution for each. The solutions of all individual problems will then be merged into a bigger proposed framework to address cyber security in Africa.

Problem 1: Lack of Focused Research in Cyber Security

This paragraph proposes a possible solution to the problem regarding a lack of research to expand the Body of Knowledge (BOK) of Cyber Security in Africa.

An African Cyber Security Centre (ACSC) for cyber prevention is proposed. The ACSC must be the central place and contact point in Africa where all aspects related to critical information infrastructure protection (CIIP) and cyber security are coordinated and where expertise and skills in these areas can be found. According to Von Solms and Kritzinger, these could include (von Solms and Kritzinger, 2010):

- Cyber security awareness,
- Capacity and skills development,
- Legislative and policy aspects,
- National computer security incident response teams (the CSIRTs),
- Research in cyber security and CIIP.

The view expressed by this research conducted by Von Solms and Kritzinger indicates that "international experiences and best practices in this area highlight one core issue, and that is **collaboration. "**Before African states start cooperating on matters such as CIIP and Cyber Security, progress will remain disjointed and incomplete" (von Solms and Kritzinger, 2010). Should such noble ideas not be implemented, Africa will, without any doubt, become a playing field for cybercrime.

The Main Focal Point of this Solution is therefore Collaboration of All Stakeholders to Establish an ACSC that will Prevent Cybercrime throughout Africa.

The recently established Centre for Cyber Security, a joint venture between the

University of Johannesburg and the UN's International Telecommunications Union (ITU), is the first step in this direction. The centre will offer a certificate in Cyber Security from middle 2012. The ITU-UJ centre for Cyber Security intends to address all the aspects mentioned above.

Another cyber initiative is the South African Cyber Security Academic Alliance (SACSAA). Three South African universities joined forces to establish the alliance. This alliance was established in June 2011. The main objective of SACSAA is to campaign for the effective delivery of cyber security awareness throughout South Africa to all groupings of the population. The founding members of SACSAA are the University of Johannesburg, the Nelson Mandela Metropolitan University and Unisa. One of the major objectives of SACSAA on the short term is to organise an annual SA Cyber Security Awareness Day – the first of which is planned for October 2012. The alliance will also invite the industry to join as members so that a comprehensive continuous national program of cyber awareness can be put into operation in South Africa. The alliance aims to create and provide workbooks that focus on improving cyber awareness amongst school learners. This workbook will be translated into a number of official languages. This workbook will be available at the end of 2012.

There is, therefore, some progression by individual groups to enhance cyber security. This is however, not enough and must have the buy-in of the relevant government departments within African countries.

Problem 2: Lack of a Proper Integrated Framework on Legal and Policy Aspects

This paragraph proposes a possible solution to the problem regarding the lack of official legislation to protect the critical infrastructure of all countries within Africa. One solution is to take the following aspects into account as Akuta, Ong'oa and Jones suggested different role players that should be involved (Akuta, Ong'oa and Jones, 2011):

- Law enforcement
- Legislators
- Anticrime commissions
- Researchers

Akuta, Ong'oa and Jones continue to state that "a shared knowledge base" as well as "law policies and practices" is vital to combat the cybercrime prevention rate (Akuta, Ong'oa and Jones, 2011).

It is clear the legal aspects of creating and implementing laws and policies which form the basis of fighting cybercrime. These are enhanced by effective research and a shared knowledge base for cybercrime prevention. Another aspect that this research enforces is the importance of involving different stakeholders and the role each one plays in cyber safety.

The Main Focus of this Approach is Identifying Different Stakeholders Involved in an Attempt to Decrease Cybercrime in Africa, as Well as Identifying Different Legislation and Policies to Support Cyber Safety.

Problem 3: Lack of Cyber Security Awareness and Regulation

This paragraph proposes a possible solution to the problem regarding how to enhance cyber security awareness and willingness to grow a cyber culture within Africa.

This solution focuses mainly on the end-users, for example home users that have little or no information security knowledge or background regarding safe cyber use.

The European Network and Information Security Agency defines a home user (HU) as "a citizen with varying age and technical knowledge who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments" (European Network and Information Security Agency, 2006). It is these home users (the public) that are currently the main concern regarding cyber incidents (in Africa as well as around the world). Kramer, Starr and Wentz have done some research on the field and had the following to say: "The sorry state of information security awareness for the public at large is an even bigger problem than the relative lack of security awareness in enterprises" (Kramer, Starr and Wentz, 2009). Kramer et al. are also supported by Kumar, Mohan and Holowezak who state that "home computers with access to the Internet are one of the weaker links as they are typically not as well protected as computers in the corporate world" (Kumar, Mohan and Holowezak, 2008).

Unfortunately, not all computer users are alert to these things. They continually use unprotected PCs as Kramer et al. observe: "The large number of users who fall for phishing scams, lack anti-malware tools, run unpatched systems, and choose easily guessed passwords for their accounts indicate that the public is either not aware of sound security practices or does not understand the threats" (Kumar, Mohan and Holowezak, 2008). It is therefore vital that HUs are assisted to connect to the web by complying with specific regulations and awareness criteria to attempt to decrease cybercrime. This is depicted in figure 1 below.

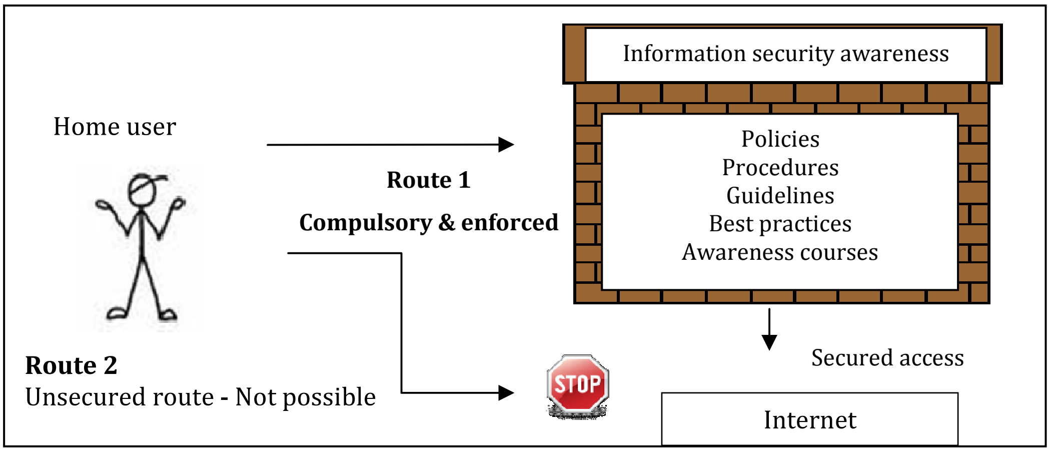

Figure 1. Cyber Safety Route (Kritzinger and Von Solms, 2010)

Figure 1 shows that the ultimate goal is to ensure that HUs are assisted through awareness to choose the route (route 1) that will provide them with more cyber safety than the unsecure route 2. This is further explained in figure 2.

Figure 2 depicts the proposed home user awareness life cycle. This process indicates the different steps a home user must follow to ensure cyber safety. HUs will not (cannot) attempt this on their own. Regulation must be implemented.

The Main Focus of this Approach is to Ensure that All Cyber Users are Exposed to Information Security Awareness Tools to Assist them to Use the Most Secure Route to Connect to the Web.

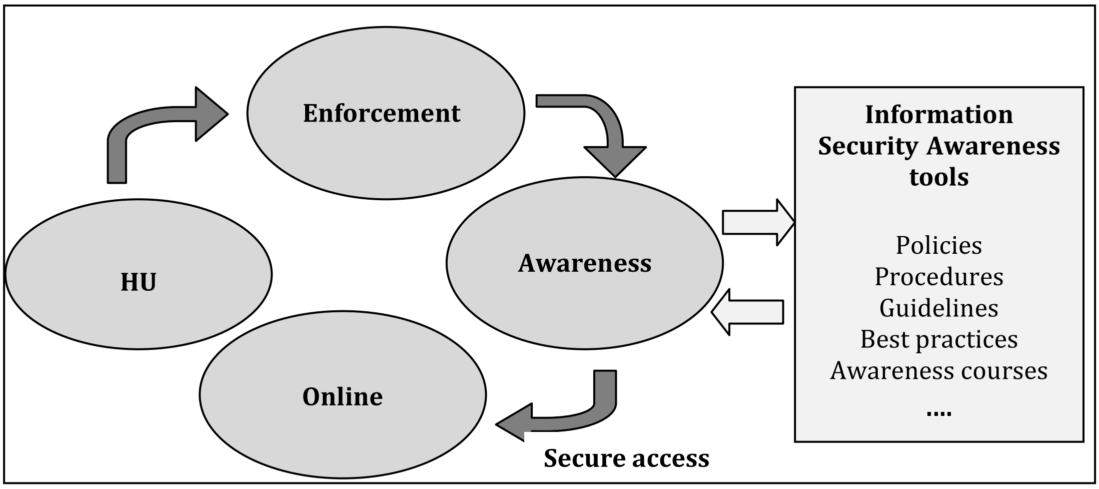

Figure 2. Home User Awareness Life Cycle (Kritzinger and Von Solms, 2010)

It is important to understand that numerous HUs will not comply with this automatically. It is therefore vital that some kind of regulation be implemented to assist HUs to complete this life cycle and become cyber safe. This regulation of cyber use is investigated in the next solutions.

Problem 4: Lack of Technical Security Measure

This paragraph proposes a possible solution to the problem regarding how to utilise a technical approach to ensure cyber safety.

This solution, which is discussed at length by Kritzinger et al. (2011), focuses mainly on using regulating bodies to assist cyber users in their responsibilities regarding cyber use. The idea of regulating bodies, for example ISPs, will help cyber users to deal with the responsibilities they are not capable of implementing. The involvement of an ISP will assist HUs with numerous responsibilities (thick HUs) to share their responsibilities (intermediate HUs) with an ISP. The ISP could also handle most of their responsibilities to ensure thin HUs. The main problem facing most home users therefore, as Schneier points out is that "Home users are on their own" (Schneier, 2007). And this is a major setback in presenting a united front to deal with cyber security. And Scheier believes, correctly so, that "it's unrealistic to expect home users to be responsible for their own security. They don't have the expertise, and they're not going to learn" (Schneier, 2007).

It should therefore be the duty of us all to help home users understand the dilemma that we are facing. As Rowe, Reeves and Gallaher make it crystal clear that "home user is not only a possible threat to themselves but also to all other users. Compromised users are starting to compromise other users for example through being a zombie computer" (Rowe, Reeves and Gallaher, 2009).

Therefore, this approach focuses on involving ISPs to assist HUs in their cyber safety. Perhaps Rowe et al. have a point when they say "ISPs are in optimal location to identify malicious incoming & outgoing Internet traffic and ISPs have knowledge and capabilities to react" (Rowe, Reeves Wood and Braun, 2010).

The reason why ISPs are so important is that any user using the internet (via a PC or mobile device) must work through an ISP to connect to the web. This move from a thick HU to a thin HU is depicted in figure 3 (revised version of Kritzinger and von Solms, 2011).

It is clear in figure 3 that the responsibilities of thick HUs will decrease and their security will increase with more involvement of ISPs.

The Main Focus of this Approach is to Incorporate the Assistance of ISPs to Assist in the Responsibilities Hus have in

Securing themselves and their Information.

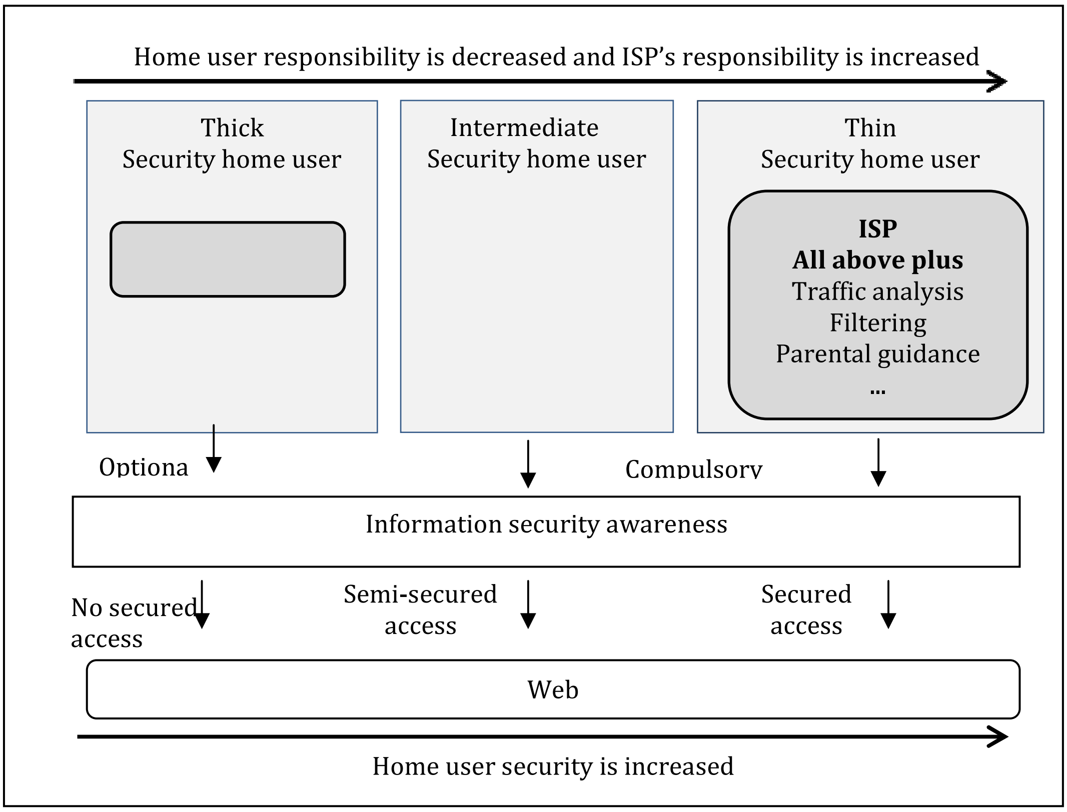

Figure 3. Security vs. Responsibility of Home User Security (Kritzinger and Von Solms, 2011)

Cyber Focus Areas

Each of the above investigated cyber solutions contributes one or more unique cyber focus aspects in the attempt to address cybercrimes in Africa. Many of these focus aspects are similar to the aspects found with developed countries and the way they handle cybercrime. The difference is that almost all African countries are developing countries and the circumstance is quite different when it comes to the implementation of the focus aspects.

There is also some overlap with some of these cyber approaches. The different cyber focus aspects include:

- Research,
- Shared common body of knowledge,
- Awareness & education initiatives,
- Technical aspects,
- Laws, legislation, best practice, etc.,
- Enforcement,
- Cyber prevention authority bodies,
- Implementation & monitoring,
- Involvement of ISPs.

The different focus aspects can be grouped together into different focus areas to form units of aspects that address the area. These different focus areas are identified in the next section that forms the basis to the proposed model to assist in the prevention of cybercrime within Africa.

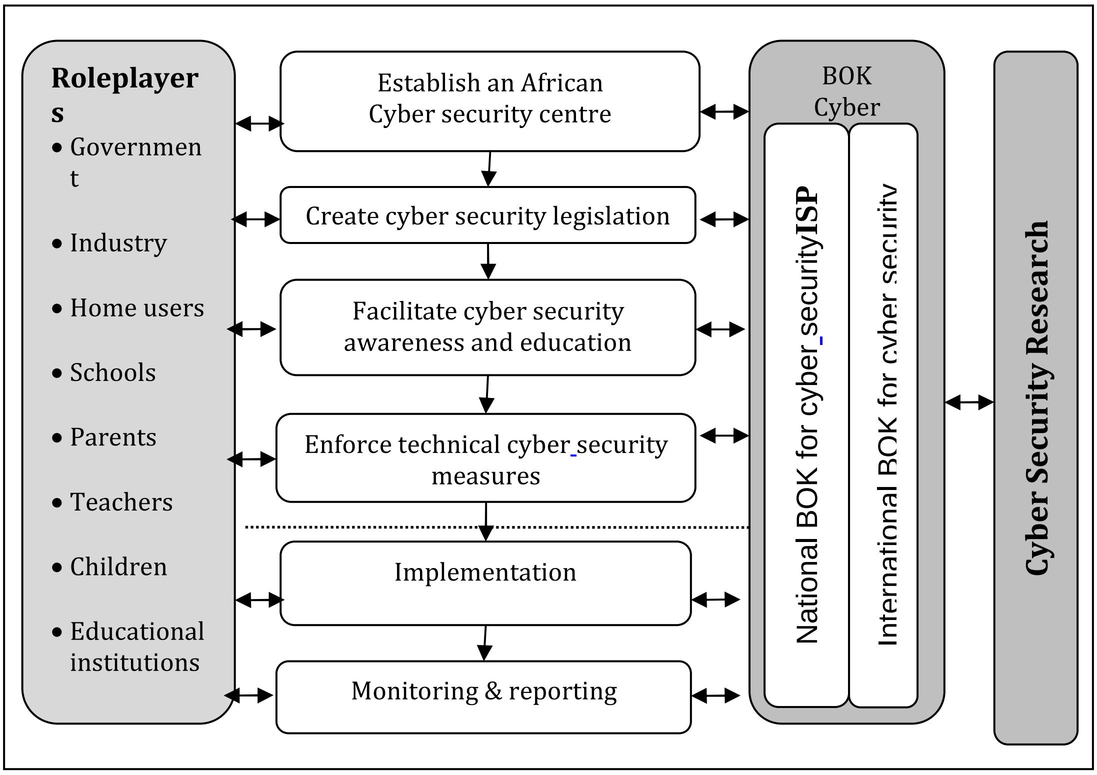
Roleplayers
• Government
• Industry
• Home users
• Schools
• Parents
• Teachers
• Children
• Educational institutions
Establish an African Cyber security centre
Create cyber security legislation
Facilitate cyber security awareness and education
Enforce technical cyber security measures
Implementation
Monitoring & reporting
BOK Cyber
National BOK for cyber securityISP
International BOK for cyber security
Cyber Security Research

Figure 4. Proposed Comprehensive Framework for Cyber Safety

Proposed Cyber Security Framework

The cyber prevention model proposed in this section comprises four dimensions vital for cyber protection. These dimensions are a combination of all the focus areas derived from the different approaches investigated in the paper. It is important to note here that these focus areas in themselves are not new and have been mentioned in literature as shown above. However, what is lacking for Africa is that these focus areas are not combined into one single implementation plan of action specific to Africa. All the above approaches are stand-alone ideas that are not currently connected or linked. It is therefore important to combine all approaches (and there are more than just mentioned in this paper) to one single action plan for cyber prevention in Africa. The different dimensional approach this paper proposes is indicated in figure 4.

The dimensions in figure 4 depict the various cyber tools needed for fighting cybercrime. There are four identified dimensions:

- Role-players
- Body of Knowledge (BOK) for cyber safety
- Cyber security research
- Cyber actions

The first is the role-players. These include all people with a role and responsibility to ensure the cyber safety of cyber users. The role-players range from government, school teachers, parents to the cyber users themselves.

The next dimension is the BOK. It is vital that there is BOK regarding cyber safety that is obtained from international (outside of Africa) sources. It is just as important to obtain (establish) a BOK for cyber safety that is built upon knowledge unique to Africa.

The third dimension is that of cyber research. It is vital that all sectors (academic, industry and government) commit to doing research to enhance the understanding and prevention of cyber safety. The research (unique to Africa) obtained through research will then form the basis for the cyber safety BOK within Africa.

The fourth dimension that is core to the proposed model is that of cyber action. This includes all actions to be taken by all role-players involved to design, approve and implement cyber security to enhance the cyber culture. Examples of these actions include:

- Creating cyber security legislation;
- Designing cyber security awareness programs;
- Monitoring and reporting of cyber threats.

One reason why this last dimension is important is that it is vital that all cyber security related measures must not only be on paper, but must be implemented amongst all cyber users. Only if cyber security becomes a reality in real life will the overall cyber culture within Africa start growing.

This will ensure that the cyber prevention initiatives are working correctly to decrease cybercrime. As mentioned above this is where the real challenge for Africa will start. Due to the different situation (for example income, education, background knowledge and experiences) of Africa, the implementation method must be Africa-specific. However, Jenson seems to be having a solution for this when he states that “the process in Africa must be tailored to such specific conditions as generally low income, limited formal business activity, the much greater importance of the rural population and small producers, and shared use of such communication resources as ...Internet accounts” (Jensen, 2011).

The same implementation of cyber crime tools used in developed countries may not always be useful in Africa. It is therefore important that all the previous steps are designed to be part of a unique Africa implementation strategy for cybercrime prevention. As an old adage says, prevention is, after all, better than cure.

From the proposed cyber prevention model, it can be clearly seen that a number of different aspects need to be included and combined to prevent cybercrime. Cybercrime cannot be prevented through stand-alone initiatives that do not form part of a properly thought out cyber prevention plan with the backing of the necessary stakeholders.

Only if Africa implements such a plan is it possible to fight cybercrime in African countries.

Conclusion

A cyber protection model was proposed to assist African countries in addressing the rapid increase in cybercrime in numerous African countries. The proposed model for Africa combines a number of approaches already established in literature. These approaches cover very valid issues regarding various aspects of cybercrime. This research therefore aims to combine different cyber prevention aspects and integrate them in a dimensional implementation plan in an attempt to decrease cybercrime in Africa.

References

Akuta, E., Ong'oa, I. & Jones, C. (2011). 'Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice,' *Journal of Peace, Gender and Development Studies* Vol 1(4) Pp129-137.

Ciso, (2009). Cisco 2009 Annual Security Report, Available at: www.cisco.com/en/US/.../annual_security_report.html.

Cole, K., Chetty, M., LaRose, C., Rietta, F., Schmitte, D. K. & Goodman, S. E. (2008). "Cybersecurity in Africa: An Assessment," Available at: http://s3.amazonaws.com/zanran_storage/www.cistp.gatech.edu/ContentPages/43945844.pdf.

European Network and Information Security Agency – ENISA, (2006). A users' guide: How to Raise Information Security Awareness, Available at: http://www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/en.

Greenwood, L. (2009). Africa's Mobile Banking Revolution, Available at: http://news.bbc.co.uk/2/hi/business/8194241.stm

Jensen, M. (2001). ICT in Africa, Online Available: http://goo.gl/mYhTR

Jensen, M. ICT in Africa – A Status Report (Chapter 6), Online available: https://members.weforum.org/pdf/Global_Competitiveness_Reports/Reports/GITR_2002_2003/ICT_Africa.pdf

Kramer, F. D., Starr, S. H. & Wentz, L. K. (2009). Cyber Power and National Security, *Center for Technology and National Security Policy and National Defence University.*

Kritzinger, E. & von Solms, S. H. (2010). "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement," *Computers & Security* Vol 29 Pp840-847.

Kritzinger, E. & von Solms, S. H, (2011). 'A New Role for Information Service Providers (Isps) as Part of Critical Information Infrastructure Protection in Africa,' CIP Report, Center for Infrastructure Protection and Homeland Security, Vol 9(12), *George Mason University, USA.*

Kumar, N. (2010). Africa Could Become the Cybercrime Capital of the World, Available At: http://www.psfk.com/2010/04/africa-could-become-the-cybercrime-capital-of-the-world.html.

Kumar, N., Mohan, K. & Holowczak, R. (2008). "Locking the Door but Leaving the Computer Vulnerable: Factors Inhibiting Home Users' Adoption of Software Firewalls," *Decision Support System* Vol 46 Pp254-264.

Rowe, B., Reeves, D. & Gallaher, M. (2009). 'The Role of Internet Service Providers in Cyber Security,' *Institute for Homeland Security Solutions.* Available at: https://www.ihssnc.org/portals/0/PubDocuments/ISP-Provided_Security_Rowe.pdf.

Rowe, B., Reeves, D., Wood, D. & Braun, F. (2010). Estimating the Market for Internet Service Provider-Based Cyber Security Solutions, Available at: https://www.ihssnc.org/portals/0/2010%20IHSS%20Research%20Summit_Rowe.pdf.

Schneier, B. (2007). Home Users: A Public Health Problem?, Schneier on Security Blog Entry Written on September 14, 2007. Retrieved April 24, 2009, at http://www.schneier.com/blog/archives/2007/09/.

von Solms, B. & Kritzinger, E. (2010). Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa – Has the CIIP and Cyber Security Rubicon been crossed? Proceedings of the AFRICOMM conference, Zanzibar.