Framework for an African Policy Towards Creating Cyber Security Awareness

IZ Dlamini[1], B Taute[2] and J Radebe[3]

[1] Defence, Peace, Safety & Security, Council for Scientific and Industrial Research, Pretoria, RSA

[2] Meraka, Council for Scientific and Industrial Research, Pretoria, RSA

[3] Cyber Security Department, Department of Communications, Pretoria, RSA

idlamini@csir.co.za

btaute@csir.co.za

jabur@doc.gov.za

Abstract: Cyber security is a GLOBAL issue. The rest of the world needs Africa to be aware and ready. Furthermore, Africa can only be aware and ready if it is internally organised and collaborates effectively with the rest of the world. The African continent consists mostly of developing countries where the needs for cyber security awareness programmes are different from developed countries. Therefore, it makes perfect sense for the continent to cooperate with respect to cyber security joint initiatives and by sharing best practice and skilled resources for cyber security awareness and response. There is currently no continental coordination of cyber security. This paper proposes a high-level African Cyber Security Policy as well as an African Cyber Security Awareness Framework to guide cyber security agencies, standards and legislation as well as specific initiatives to promote cyber security awareness. This is achieved through the analysis of a few Cyber Security Policies from developed countries (USA, UK, Estonia, Korea), identification of African countries that have such policies in place, and identification of the agencies, forums, workgroups, conferences, organisations and other initiatives that are currently dealing with ICT and cyber security policy and awareness in Africa – including ITU, Interpol, AfriNIC, ISG-Africa and country-specific organisations such as Computer Security Incident Response Teams.

Keywords: cyber security, awareness, policy, Computer Security Incident Response Teams, Computer Emergency Response Team, agencies

1. Introduction

Cyber security has become a GLOBAL issue of concern, judging from the increase in importance it has received in the developed world (USA, UK, Estonia, Europe, Korea and others) where national cyber security strategies have been developed in response to increased cyber crime and attacks. The rest of the world needs Africa to be aware and ready since we are all connected in cyber space and our collective security is linked through either being hosts or targets of crime and attacks. Furthermore, Africa can only be aware and ready if it is internally organised and collaborates effectively with the rest of the world. Currently, the African continent is particularly vulnerable to cyber security threats largely because of vastly increased bandwidth that is bridging the "digital divide" for economic and social reasons; and becoming available to areas where dial-up connections

were the norm and where the IT literacy levels are varied and sometimes very low. This is growing fast through wireless networks (lacking cable infrastructure in some areas) and mobile phones that are for many the first and primary access to the internet. These factors increase the vulnerability to malware infection, cyber bullying via social networks, cyber abuse of children, cyber terrorism and the risk of hosting malicious hackers.

The continent which consists mostly of underdeveloped and developing countries is characterised by a limited awareness, knowledge, expertise and understanding of cyber security [1]. Some of the reasons that have been cited for this lack of security awareness include shortage of local cyber security experts, and the lack of funds, just to mention a few.

So far only a handful of countries in Africa have been working towards a national cyber security policy. As it will be shown, only one of which explicitly focuses on awareness. At the same time, there are various agencies and organisations involved in African cyber security activities. In view of the limited capabilities and resources, and taking advantage of the current digital "wave", the African continent needs to be aware and be prepared to identify and mitigate the cyber security vulnerabilities and threats through joint initiatives, sharing best practices and skilled resource by:

- Collaboration with international role players.
- Continental collaboration on cyber security awareness at political, business, policing, education and society levels, guided by an African Cyber Security Awareness Framework and facilitated by appropriate continental organisations.
- African Cyber Security Awareness workshops, programmes, conferences, training courses and other initiatives – both new ones and building on existing initiatives.

Globally there is a renewed focus on cyber security (e.g. the National Cyber Security Awareness Month declared by the President of the USA, October 2010) due to the increased frequency, sophistication and scale of malware infection and attacks from hackers, criminals and cyber terrorists on government, business, critical infrastructure and citizens [2]. The paper proposes the African Cyber Security Awareness Framework that is flexible to be adapted into any country's cyber security policy as well as specific initiatives promoting cyber security awareness in the continent of Africa [3]. A cyber security awareness framework is seen in the context of a broader cyber security policy.

This paper starts by describing the cyber security landscape in Africa by reviewing the security policies that exist and identifying workgroups or organisations that are currently dealing with cyber security in Africa. This is followed by an analysis of a few Cyber Security Policies from developed countries namely, US, UK, Estonia, and Korea, to be used as a point of reference and a benchmark for the development of the proposed framework. The review will analyse the extent to which these policies address awareness as well as related issues such as education, support to industry and citizens, collaboration and increase in technical expertise, and linkages with global initiatives such as the EU Convention on Cyber Crime. On the basis of the above, the paper proposes a high-level blueprint for an African Cyber Security Policy, and as part of an African Cyber Security Policy, the view is narrowed to cyber security awareness programmes in Africa.

2. African Cyber Security Policies and Organisations

This section is presented in two parts. The first part identifies continent level cyber security role players in Africa and the second part reviews the South African, Mauritian, Kenyan and Tunisian cyber security policies.

2.1 Cyber Security Role-Players on the African Continent

The following gives a brief summary of role players and what they do.

The United Nations Economic Commission for Africa (UNECA) is addressing cyber security within the framework of the African Information Society Initiative (AISI) [5]. The establishment of the necessary cyber security organisational structures with national responsibility, including national computer incident response teams (CIRTs) is still at construction level. These national efforts can at the same time initiate cooperative activities at the continental and international levels, with the possible establishment of regional centres.

According to UNECA, African governments are demonstrating increased awareness of cyber security issues, but existing capability to promote, monitor or pursue cyber security is relatively low [5]. Some countries in the region, namely Burkina Faso, Burundi, Cote D'Ivoire, Egypt, Iraq, Kenya, Mauritius, Morocco, Nigeria, Rwanda, Saudi Arabia, South Africa, Tanzania, Tunisia, Uganda, United Arab Emirates, and Zambia, are now working with ITU, in collaboration with key partners, such as the International Multilateral Partnership Against Cyber Threats (IMPACT), to facilitate the development of cyber security capabilities, including the establishment of national CSIRTs [6].

Some of the key player organisations on the African cyber security issues are as follows:

- **International Telecommunication Union (ITU):** has a fundamental role to build confidence and security in the use of Information and Communication Technologies (ICTs) internationally. At the World Summit on the Information Society (WSIS), the Heads of States and world leaders entrusted ITU to take the lead in coordinating international efforts in the field of cyber security, as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs". According to [7], the ITU cyber security related resolutions include:
    - ITU Plenipotentiary Resolutions: 130, 174 , 181 (Guadalajara, 2010),
    - ITU WTDC Resolutions: 45 , 69 (Hyderabad, 2010),
    - ITU WTSA Resolutions: 50, 52, 58 (Johannesburg, 2008).
- The ITU Secretary-General, Dr. Hamadoun I. Touré launched a framework for international cooperation aimed at enhancing confidence and security in the information society, called Global Cybersecurity Agenda (GCA) [7].
- **International Criminal Police Organization (Interpol):** is the world's largest international police organisation that facilitates cross-border police co-operation, further supports and assists all organisations, authorities and services whose mission is to prevent or combat international crime. INTERPOL created its Information Security Incident Response Team

(ISIRT) in response to the increasing number of the targeted cyber attacks and information leakages. Part of the needs that are associated with cyber crime, on its 5th Meeting of the Interpol Working Party on IT Crime [8], Interpol acknowledged awareness throughout police hierarchies and political decision makers as significant.

- **African Network Information Centre (AfriNIC):** as an initiative on African cyber security, AfriNIC has established the AfriNIC Government Working Group (AfGWG) initiative with the first round table for Law Enforcement Agencies on the theme of African Inter-Governmental Coordination and Cooperation for a Safer Internet which took place 25-26 January 2010, in Mauritius [9]. AfGWG is tasked to raise awareness among African government and regulators on internet governance matters with a high emphasis on Cyber Security. There were a further two Law Enforcement workshops on CyberCrime and Cyber Security last year (2010) which are developing the African Cert Association (AfCERT). The AfCERT has held a 6 day workshop during the AfriNIC-14 meeting in Dar-Es-Salam in cooperation with JPCERT (Japan Cert), while the AfriNIC-13 meeting that was held in Johannesburg also discussed cyber security issues.

- **Information Security Group of Africa (ISG-Africa):** has partnered with various local and international agencies and organisations to help combat the massive increase in cyber crime, among other things by launching the eCrime Portal (http://www.ecrime.org.za). ISG Africa was created in response to the increase of information security threats facing companies in Africa. It consists of security professionals from corporate, government and IT or legal firms within Africa. ISG-Africa aims to provide a monthly forum for the exchange of Information Security related information and experience between members and further raise awareness of potential and identified vulnerabilities [10]. ISG-Africa has active user groups in South Africa and Nigeria (www.isgafrica.org).

- **Southern African Development Community (SADC):** mission is to promote sustainable and equitable economic growth and socio-economic development through efficient productive systems, deeper co-operation and integration, good governance, and durable peace and security. The proposed regional priorities for 2011-2012 includes, amongst others, the setting up of National and Regional Internet Exchange points; harmonisation of Cyber Security Regulatory Frameworks in SADC [11].

There are other workgroups and organisations that exist within Africa which work on cyber security and related fields, that is, IST- Africa, Africa CRYPT and African CERT, to mention the few. The African Cyber Security Awareness Framework must be able to assist African countries to collaborate on the continental cyber security awareness processes at political, business, police, education, and society levels; and further be facilitated by appropriate continental cyber security organisations.

2.2 Cyber Security Policies on the African Continent

Having national frameworks, policies and strategies related to cyber security are imperative for African countries, because they allow stakeholders (citizens, industry and governments) to use all the technical, legal and regulatory tools available to promote a culture of cyber security and its related concerns. This section gives a high-level review of the South African, Mauritian, Kenyan and

the Tunisian cyber security policies.

2.2.1 South African National Cyber Security Policy

The first draft of the South African National Cyber Security Policy was published for comment in February 2010 [12]. This draft included cyber security awareness as part of the role of the proposed National CSIRT. The content of the SA cyber security draft entailed the following headings:

1. *Legislative Framework*
2. *Policy Objectives*
3. *Creating Institutional Capacity to Respond to Cybercrime and Threats*
    - National Cybersecurity Advisory Council
    - Computer security incident response teams (CSIRTs)
4. *Reducing Cybersecurity Threats and Vulnerabilities*
5. *Coordinate Local and International Partnerships*
    - Forster cooperation and coordination between government, private sector and citizens
    - Promote and strengthen international cooperation
6. *Continuous Innovation, Skills Development and Compliance*
    - Promote compliance with appropriate technical and operational cyber security standards

South Africa is further recognised with its own Electronic Communications Security - Computer Security Incident Response Team (SA- ECS-CSIRT). The ECS-CSIRT is the South African National government CSIRT. Its constituency is the whole South African governmental organisation cyber-community [12].

2.2.2 Mauritius National Cyber Security Policy

Mauritius has most of the cyber security infrastructures in place. For example; there is Computer Emergency Response Team (CERT-MU) and Computer Incident Response Team (CIRT), Cyber Security Awareness Portal [14], and National Cybercrime Prevention Committee (NCPC). The issues that are addressed by the cyber security strategy include:

1. *National Awareness Programs and Tools*
    - MySecureCyberspace—The Portal
    - Privacy Bird and Privacy Finder
    - MySecureCyberspace—The Game
2. *Good Governance of Cyber Security & Privacy*

3. *Harnessing the Future to Secure the Present*
    - Premier centre for cyber security, dependability and privacy
    - Unique comprehensive approach
    - CyLab engages in numerous partnerships and educational initiatives throughout the world
    - Benefits of CyLab Partners Program
4. *Personal Cyber Security*
    - Home PC Security
    - Password Security
    - Child Safety Online
    - Social Engineering
    - Identity Theft
    - Road Warriors
    - Email Security
5. *A holistic approach integrates many elements*
    - Both strategic and tactical,
    - Both technical and non-technical
    - Both professional and public [15].

2.2.3 Kenyan National Cyber Security Policy

Kenya does not have national cyber security policy in place either, but has proposed to have one which will include the following topics:

1. *Collaboration between stakeholders;*
2. *Develop relevant Policies, Legal and Regulatory frameworks*
3. *Establish national CERT thus providing a Trusted Point of Contact (TPOC);*
4. *Build Capacity: technical, legal and policy;*
5. *Awareness creation is key;*
6. *Research and development;*
7. *Harmonization of Cybersecurity management frameworks at the regional level (at the very least) [16].*

The Kenya Computer Security Incidence Response Team (KE-CSIRT) has been established [17].

2.2.4 Tunisian National Cyber Security Policy

Tunisia has only proposed what will be included in their cyber security policy, but it has not been implemented yet [18]. Tunisia has both a Tunisian Computer Emergency Response Team (tunCERT) and a Computer Emergency Response Team – Tunisian Coordination Center (CERT-TCC).

When looking at the reviewed countries' policy information, the most advanced country on this issue is Mauritius. Beside Mauritius, South Africa, Tunisia and Kenya are also actively working on their laws while others are putting their cyber security policies together. It is by no doubt then that, there is still an overall lack of security awareness and understanding of cyber security in Africa. Some of the challenges that are faced include: the lack of awareness and the shortage of local experts in the cyber security field. All the countries are willing to cooperate globally on the security of cyber space, but it is necessary to collaborate regionally and learn from each other as well. An African cyber security policy will be one step forward.

3. Cyber Security Policies from Some Developed Countries

This section reviews and discusses cyber security policies of developed countries as a benchmark for the development of the proposed framework for Africa. The countries that were targeted include: UK, USA, Estonia and Malaysia.

3.1.1 UK National Cyber Security Policy

In the framework of the UK cyber security Strategy, the changes in the way things used to be done were introduced as part of the broader agenda to modernise and transform the UK government. This is said to work to modernise UK's security policy (its review is presented in Table 1) and the related processes which are all set to continue to raise awareness, ensure that guidance is up to date, that policy reflects changes in threat and circumstances, and that all government departments are supported from the centre.

The education, training and awareness MANDATORY REQUIREMENT 48 states that, the "*…departments and Agencies must ensure that all users of ICT systems are familiar with the security operating procedures governing their use, receive appropriate security training, and are aware of local processes for reporting issues of security concern…*" [4]. This requires that the staff who manage and maintain the secure configuration of ICT systems, and those with access to information assets, are appropriately trained, and are aware of incident reporting and the minimum standards relating to the handling of protectively marked data [4].

3.1.2 USA National Cyber Security Policy

The first thing the USA president, Barack Obama, did after taking over in 2009, was to make cyber security one of his top priorities, quoted during the United State of the Nation address (May 29, 2009): *"And that's why shortly after taking office I directed my National Security Council and Homeland Security Council to conduct a top-to-bottom review of the federal government's efforts to defend our information and communications infrastructure and to recommend the best way to ensure that these networks are able to secure our networks as well as our prosperity"* [22].

Table 1: Summary of the National Security Policies from Some of the Developed Countries

Country	Topics Included	International CERTs [27]
United Kingdom (UK) [19]	**Workstream 1:** Safe, Secure and Resilient System **Workstream 2:** Policy, Doctrine, Legal and Regulatory issue **Workstream 3:** Awareness and Culture Change **Workstream 4:** Skills and Education **Workstream 5:** Technical Capabilities & Research and Development **Workstream 6:** Exploitation **Workstream 7:** International Engagement **Workstream 8:** Governance, Roles and Responsibilities	**Global- CERT™** • US- USCERT • Australia- AusCERT • UK- UKCERT • Canada- CanCERT • Japan- JPCERT • Hong Kong- HKCERT **Sector specific UK CERTs** • Academic • Military • Governmental **Sector specific US CERTs** • Energy • NASA • Military **Other CERTs** • CERT-China • CERT-Croatia • CERT-France • CERT-Germany • CERT-Italy • CERT-Denmark • CERT-Finland • CERT-Korea • CERT-Lithuania • CERT-Mexico • CERT-Netherland • CERT-Norway • CERT-Poland • CERT-Russia • CERT-Slovenia • CERT-Spain • CERT-Sweden • CERT-Switzerland
United States of America (USA) [20]	• **Leading from the Top:** • Anchor Leadership at the White House • Review Laws and Policies • Strengthen Federal Leadership and Accountability for Cyber Security • Elevate State, Local, and Tribal Leadership • **Building Capacity for a Digital Nation** • Increase Public Awareness • Increase Cybersecurity Education • Expand Federal Information Technology Workforce • Promote Cyber Security as an Enterprise Leadership Responsibility • **Sharing Responsibility for Cyber Security** • Improve Partnership Between Private Sector and Government • Evaluate Potential Barriers Impeding Evolution of Public-Private Partnership • Partner Effectively With the International Community • **Creating Effective Information Sharing and Incident Response** • Build a Framework for Incident Response • Enhance Information Sharing To Improve Incident Response Capabilities • Improve Cyber security Across All Infrastructures • **Encouraging Innovation** • The Future • Link R&D Frameworks to Infrastructure Development • Link R&D Frameworks to Infrastructure Development • Integrate Globalisation Policy with Supply Chain Security • Maintain National Security/Emergency Preparedness (NS/EP) Capabilities • **Action Plans**	
Estonia [21]	**1. Threats in cyberspace** • Cyber attacks against the critical infrastructure. • Cyber crime. **2. Fields of activity supporting cyber security: Description and analysis** • Estonian information society and information infrastructure • Information system security • Training in the field of information security • Cyber security and the legal framework • International law • National legal framework	

Country	Topics Included	International CERTs [27]
	• International co-operation **3. Enhancing cyber security in Estonia: Goals and measures** • Development and implementation of a system of security measures Increasing competence in information security • Development of a legal framework for cyber security • Development of international co-operation • Raising awareness of cyber security **4. Implementation of the Strategy**	
Malaysia [18]	**THRUST 1:** Effective Governance **THRUST 2:** Legislative & Regulatory Framework **THRUST 3:** Cyber Security Technology Framework **THRUST 4:** Culture of security and Capacity Building **THRUST 5:** Research & Development Towards Self-Reliance **THRUST 6:** Compliance and Enforcement **THRUST 7:** Cyber Security Emergency Readiness **THRUST 8:** International Cooperation	

With respect to cyber security awareness programmes, increased public awareness on cyber security issues, and fostering and funding cyber security research are included in the US national cyber security policy (in Table 1). Some of the most controversial parts of the bill include Paragraph 315, which grants the President the right to "order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network [20].

3.1.3 Estonian National Cyber Security Policy

Immediately after the cyber attack that took place in Estonia, in the year 2008, the national cyber security strategy document (summarised in Table 1) was formulated to avoid future damages. As part of Estonian cyber security strategic objectives the following are some of the identified policy fronts:

- development of Estonia's expertise in and high awareness of information security to the highest standard of excellence; and
- promoting international cooperation aimed at strengthening global cyber security [23].

The following methods are used when raising public awareness of the cyber threats in Estonia:

- The presentation of the Estonia's expertise and experience in the area of cyber security at both the domestic and international level, and supporting co-operative networks;
- To raise awareness of cyber security among all computer users with particular focus on individual users and SMEs by informing the public about threats existing in the cyberspace

  and improving knowledge on the safe use of computers;
- To co-ordinate the distribution of information on cyber threats and organising the awareness campaigns in co-operation with the private sector.

There has not been any further major threat or attacks that were reported after the release of the national cyber security policy (with the presumption that the policy has been successfully implemented).

3.1.4 Malaysian National Cyber Security Policy

The Malaysian national cyber security policy is to ensure that the critical national information infrastructures are kept secured, resilient and independent, and further to promote stability, social well-being and wealth creation. One of the sections, THRUST 4 of the Malaysian national cyber security policy (refer to the summary in Table 1) discusses the development, promotion and maintenance of the national culture of security. This is to standardise and coordinate cyber security awareness and education programmes across all elements of the Critical National Information Infrastructure (CNII). The plan is to establish an effective mechanism for cyber security knowledge dissemination at the national level and to identify minimum requirements and qualifications for information security professionals [18].

Most of the developed countries specify that international cooperation in cyber security needs to be promoted in order to strengthen global cyber security [21]. This cooperation requires each country to have a readily available cyber security policy as basis. This could hinder immensely within the African countries, as only few have such a policy in place. Below is the analysis of some of the cyber security policies for the developed countries.

3.2 Analysis of Cyber Security Policies from Developed Countries

This subsection compares the policies discussed in subsection 3.1 and summarised in Table 1. Both the similarities and the differences are outlined, with a view to formulate a framework for cyber security policy within the African context.

All the policies from the developed countries are in favour of a pro-active approach in response to cyber security attacks and threats. This has resulted in each country implementing national CERTs that work collaboratively with other CERTs in order to be continuously alert and have a proactive strategy. Some of the significant noted similarities include the investment of all these countries into building individual nation's capacity on cyber security skills, though training, education and awareness programs. International cooperation is also valued by each and every one of these countries. This cooperation realises the borderless nature of cyber space and requires global engagement by ensuring that related policies and strategies are in place. Moreover, each country specified the governance of their information and systems through relevant laws, standards and regulations.

Besides these similarities, there are a few differences which distinguish some of the countries from each other. At a high level, some of the countries, that is, the UK and Estonia do not refer to these documents as policies, rather as strategies which mean that the focus is on implementation. However, apart from some differences in structuring and wording, these policies largely point to the same issues and activities that are needed to secure cyberspace. The implementation of these policies within the stated developed countries has been in place for a while and provides a basis for achieving the underlying objectives for which these countries develop their policies.

3.3 Conceptual Framework for an African Cyber Security Policy

Using the previous reviews of international cyber security policies, a conceptual framework for an African cyber security policy is tabulated in Table 2. The proposed framework combines the key points from other strategies in an intuitive way since it is not really possible to "test" the effectiveness of these policies with the available data. For a coordinated approach, this policy must have one clear vision for cyber security in Africa.

Table 2: Proposed Conceptual Framework for African Cyber Security Policy

Clause Number	Clause Name and Description
1	**Improved and Effective Information and Communication Technology Governance** • Establish cyber security leadership and accountability structures • review of laws and relevant policies – seek continental synergies to facilitate collaboration on security and combating crime • development of legislative and legal frameworks for cyber security • elevate international, regional and national cyber security leadership including the adoption of the EU Convention on Cyber Crime • establish and mobilise public and private partnerships for enhanced security • promote compliance to cyber security standards and best practices
2	**Cyber Security Awareness** • support public, business and political awareness programs • instil cyber security education from first grades at school • this is a technical function of the national CERT
3	**Formal Training** • promote cyber security skills training at universities • promote African cooperation on training programmes
4	**Improve and Maintain Crime and Incident Response** • establish world-class crime intelligence, investigation, forensics and enforcement • support formulation of regional, national and sector CSIRTs/CERTs • promote public and private sector partnerships for response • promote national and continental readiness and action plans • international cooperation with other CERTs • programmes to protect critical information, infrastructure and systems
5	**Technological Governance** • digital device use, and exploitation, e.g. governing of mobile phone and wireless security • develop technological policies and relevant standards for the safe use of cyber space • implement security by design
6	**Research, Development and Innovation on Cyber Security** • research to ensure security of critical information infrastructures • review and maintenance of up to date cyber security standards • keep national emergency responsiveness up to date and maintained • proactive research on securing the internet of the future • encourage innovation and growth in the cyber security industry

Clause Number	Clause Name and Description
7	**Globalisation** • establish continental forum(s) for cyber security collaboration • harmonise legislation and adopt the EU Convention on Cyber Crime • participate in global cyber security initiatives

Apart from setting the vision for African cyber security the following issues need to be addressed:

The *goal* for cyber security in Africa should be to enable the full benefits of cyber space to all African countries while investing in human capacity development of all the citizens. The main *objectives* for cyber security in Africa could be online security of the African cyber space by improving knowledge, capabilities and decision making. The *legal issues* on the management and governance of the policy should be equally chaired by the representatives from participating countries. Furthermore, the *technical content* of the policy should be thoroughly investigated and agreed upon by all countries.

A key point is that the African continent is collectively vulnerable and that no country can do it alone. Similarly, the proverbial weakest link can affect all countries. Therefore, it is imperative that countries more advanced in cyber security should assist the others, and the African policy should include raising the level of skills, institutions and awareness in all countries while learning from and collaborating with the rest of the world as well. Due to the similar conditions in African countries, best practices from neighbours will be more relevant than best practice from already developed countries.

Moreover, the framework from Table 2 is at a basic level to form a basis for future work. It is presented at a practical level. The following section discuses cyber security awareness programmes in more detail.

4. Cyber Security Awareness Programmes

According to UK's HMG Security Policy Framework [4], it is governments' role to raise cyber security awareness within the country. Awareness is used to stimulate, motivate, and remind the audience what is expected of them [24]. This is an important aspect of cyber security policy because it enhances security knowledge of users, changes attitude towards cyber security, and changes behaviour patterns. These factors improve the resilience of users against cyber attacks. Cyber Security Awareness is a well-developed field of study; therefore this article makes use of best practice insights from existing programmes.

Peltier believes that a cyber security awareness program has five key elements that must be presented to the audience [24]. These include:

- A process to take the message to the user community in order to reinforce cyber security as a significant concept.
- Identifying the individuals who are responsible for the implementation of the security program.

- Determine and evaluate the sensitivity of information and the criticality of cyber security infrastructure, applications and systems.
- The reasons for the implementation of cyber security concepts and awareness programs in convincing the participants of the significance of cyber security awareness programs that must be implemented.
- Ensure that the related government department supports the goals and objectives of the cyber security program of the community.

The following statistical information is typical of many countries and a strong part of the motivation for Cyber Security Awareness Programmes (CSAP).

In South Africa (SA), the study conducted by [10] in Port Elizabeth on 1594 children from grades 6 to 12 resulted in the following statistics:

- Average of 83% had a household PC,
- Average of 75% had internet access,
- Average of 60% knows how to delete their internet history,
- Average of 65% do not have to ask anyone for permission to access internet,
- Average of 50% use internet for social engineering purposes,
- 42% of teenagers have been cyber bullied,
- 53% of kids admit to saying something hurtful online,
- 58% of kids did not report an incidence of cyber bullying to an adult,
- Victims of cyber bullying are twice as likely to attempt suicide [10].

In order to mitigate some of the stated problems and risk areas, the framework for CSAP (depicted in Figure 1) provides a basis for organising such campaigns within a country. The national cyber security policies, legislation, procedures, laws and standards should serve as the foundation where CSAPs will be built upon [25].

The CSAP framework further suggests that Planning, Designing, Implementation and Evaluation processes should be continuous. Since the cyber security awareness programmes are cyclic processes, the four processes should also use the same cyclic pattern [26]. The following components constitute the process of formulating cyber security awareness programmes:

- *Security Awareness Goals and Objectives:* this must be defined in terms of the national legislation, laws, policies and standards as well as continental policies and agreements.
- *Identify Current Training Needs:* see Figure 1.
- *Obtain Support:* see Figure 1.

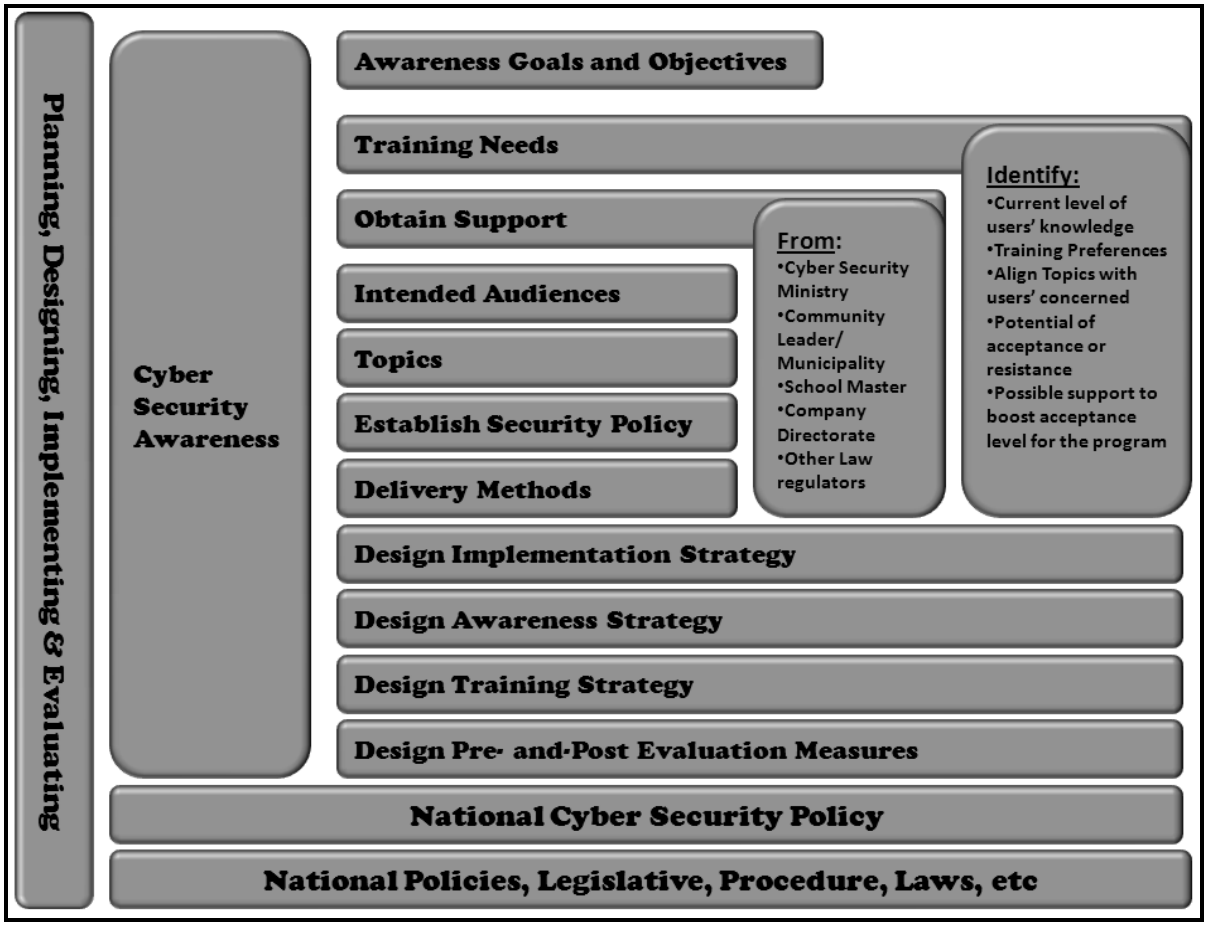

Figure 1. Proposed Cyber Security Awareness Framework

- *Identify Intended Audience:* these are the target trainees, to whom cyber security awareness programmes will be delivered (e.g. community citizens, IT employees, non-IT employees, students, learner, etc.).
- *Define Topics to be covered:* the list of topics must be evaluated in terms of relevance to each targeted audience.
- *Establish Security Policy*: this policy will state the governance of all security related assets, devices, and infrastructures to assist in governing all cyber security related gadgets.
- *Define Delivery Methods to be used*: this includes the way in which the CSAP will be presented to different audiences (e.g. primary learner: use cyber security posters and drawings, employees: use emailing system, company news letter, seminars, etc.).
- *Develop a Strategy for Implementation*: this should be decided on all levels and the entire programme should be evaluated for possible loopholes (e.g. the programmes implementation should start from the grade zero, in schools; or the arrangement of the seminars in the workplace, that is, which group attends it first in order to avoid disturbing all the company duties).

- *Design Awareness Strategy*: this includes the smaller details of the awareness programmes (e.g. how can the audience be kept attentive or how they can be attracted to these programmes).
- *Design Training Strategy*: this may include the alignment of the trainer, the venues, etc.
- *Develop Evaluation Methods*: these are the methods that will be used to test the effectiveness of the cyber security awareness programmes (e.g. comparison of pre- and pos-survey).

Further developments on CSAP in Africa may include: African Cyber Security Awareness workshops, programmes, conferences and training courses. These initiatives are sought to implement cyber security awareness at the continental level.

5. Conclusion

While the rest of the world is increasing its focus on cyber security through relevant policies, strategies, infrastructure, technology development and awareness campaigns, only a few African countries have cyber security policies and appropriate security response structures or agencies such as CERTs. This is despite the fact that the African continent is today especially vulnerable to cyber attacks due to unique problems within the developing context. These problems include bridging the digital divide, dealing with low levels of IT literacy, the dominant use of mobile devices and wireless networks, and the challenges brought on by the current roll-out of broadband internet access.

This paper proposed a high-level framework for an African cyber security policy as well as a framework to initiate and maintain awareness programmes. This is based on a literature study followed by interpreting and combining the information from available policies. The proposed African policy addresses country-specific as well as continental ICT governance, security awareness, training, incident response, technology governance, globalisation and research and development. An African cyber security policy and strategy may take a long time to develop and indeed struggle to find the appropriate organisations and prioritised attention for development. However, awareness campaigns should not wait for continental strategies. Fortunately, there are already a number of organisations that have identified the need for continental coordination and increased cyber security awareness – including UNECA/AISI, AfriNIC, ITU/GCA, Interpol, SADC and ISG-Africa. These organisations should be supported with achieving their objectives regarding cyber security awareness in Africa.

Cyber security awareness should reach all levels and inform all users of the internet – from vulnerable, school-going children to families, industry, critical national infrastructures, governments and the African continent with its unique needs. This will enhance resilience against cyber crimes and attacks and inform African policy development but also prompt the establishment of appropriate organisations such as CSIRTs and collaboration mechanisms to secure the continent and join the efforts of the global community of responsible and secure internet users.

References

[1] e4Africa, 2011. Technology in schools – for better or for worse, available online from: http://www.e4africa.co.za, Accessed on [03 February 2011].

[2] C. McCoy, R.T. Fowler, ""You are the key to security": establishing a successful security awareness program", Proceedings of the 32nd annual ACM SIGUCCS conference on User services, pp.346-349, 2004.

[3] Burgos, D., Tattersall, C., et al. "Re-purposing existing generic games and simulations for e-learning. Computers in Human", 2007.

[4] HMG Security Policy Framework, http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-security-policy_0_0.pdf

[5] African Union Summit, 2010, Division of Communication And Information, ICT In Africa – Information Sheet N6, Cyber Security, available online from: http://www.pdfcari.com/pdf/ICT-Security-Africa-Summit-2010.html, Accessed on [05 February 2011].

[6] ITU, ITU Regional Cybersecurity Forum 2009, Tunisia, available online from: http://www.itu.int/ITU-D/cyb/events/2009/tunis/index.html, Accessed on [15 February 2011].

[7] ITU, ITU Activities related to Cyber security, available online from: http://www.itu.int/cybersecurity/, Accessed on [01 March 2011].

[8] Interpol, Resolution of the Delegates, available online from: http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Africa/5thMeeting/Resolution.asp Accessed on [13 March 2011].

[9] AfriNIC, African Inter-Governmental Coordination and Cooperation for a Safer Internet, available online from: http://www.afrinic.net/press_release_le_050210.htm, Accessed on [23 February 2011].

[10] ITWeb, ISG Africa launches eCrime Portal, available online from: http://www.itweb.co.za/office/isgafrica/PressRelease.php?StoryID=205555, Accessed on [09 March 2011].

[11] SADC, Meeting of SADC Ministers Responsible for Telecommunications, Postal and ICT, available online from: http://www.sadc.int/index/browse/page/750, Accessed on [11 March 2011].

[12] SA government gazette, 2010. South African National Cybersecurity Policy, available online from: http://www.pmg.org.za/files/docs/100219cybersecurity.pdf, Accessed on [02 March 2011].

[13] South Africa, South African Computer Security Incident Response Team (ECS-CSIRT), available online from: http://e-comsec-com.win7.wadns.net/ECSCSIRT/tabid/109/Default.aspx, Accessed on [07 March 2011].

[14] Mauritius Cyber Security Awareness Portal, available online from: http://www.itu.int/wsis/stocktaking/plugin/listing.asp?lang=en&c_from=|MAR&c_from_text=Mauritius, Accessed on [23 February 2011].

[15] Carnegie Mellon_ CyLab, 2008. Message from Mauritius (Part II): Holistic Cyber Security Strategy -- Professional & Personal, available online from: http://www.gov.mu/portal/sites/csd/downloads/ppt/Track3/Mauritius.pdf, Accessed on [13 March 2011].

[16] Ngundi, V. 2010. Cybercrime, Cybersecurity and Privacy, available online from: http://www.eaigf.or.ke/files/2010_KIGF_Cybercrime_Cybersecurity_and_Privacy.pdf, Accessed on [05 March 2011].

[17] Kandiri, J.M. ICTPolicy In Kenya And Ways Of Improving The Existing ICT Policy, available online from http://www.strathmore.edu/rso/research/ict-policy-in-kenya.pdf, Accessed on [09 February 2011].

[18] MOSTI, 2009. National Cyber Security, the way forward, available online from: http://www.mosti.gov.my/mosti/images/pdf/national_cyber_security.pdf, Accessed on [01 March 2011].

[19] Cabinet Office, 2009. Cyber Security Strategy of the United Kingdom, available online from: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf, Accessed on [20 February 2011].

[20] Cyberspace Policy Review, Assuring a Trusted and Resilient Information, Accessed on [12 February 2011] and Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[21] Ministry of Defence-Estonia, 2008. Caninet Office, 2009. Cyber Security Strategy- Cyber Security Strategy Committee, available online from: http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf, Accessed on [23 February 2011].

[22] Obama, B.H. 2009. Remarks By The President On Securing Our Nation's Cyber Infrastructure, BH Obama, President of the United States of America; The White House, Office of the Press Secretary, available online from: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/, Accessed on [21 February 2011].

[23] Osrin.net, 2011. Estonia's Cyber Security Policy, available online from: http://osrin.net/2008/10/estonias-cyber-security-policy/, Accessed on [28 February 2011].

[24] T. Peltier, "Implementing an Information Security Awareness Program". Information Systems Security 14. Vol. 2, pp. 37–49, 2005.

[25] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study ", Journal Computers & Security, vol. 4, pp. 12-25, 2005. Vol 27, pp 241-253, 2008.

[26] B.D. Cone, C.E. Irvine, M.F. Thompson and T.D. Nguyen, "A video game for cyber security training and awareness", Journal Computers & Security, vol. 16, pp. 63-72, 2007. Vol 27, pp 241-253, 2008.

[27] UKCERT, 2011. United Kingdom Computer Emergency Response Teams, available online from: http://www.ukcert.org.uk/, Accessed on [24 February 2011].