Information & Security: An International Journal

Okuku, Renaud & Valeriano, vol.32, 2015 http://dx.doi.org/10.11610/isij.3207

CYBERSECURITY STRATEGY'S ROLE IN RAISING KENYAN AWARENESS OF MOBILE SECURITY THREATS

Angela Okuku, Karen Renaud, and Brandon Valeriano

Abstract: Cybersecurity has become a global concern, particularly in rapidly developing countries like Kenya. Kenya's ICT revolution followed the laying of undersea cables in 2009. Kenya's growth in Internet use has been facilitated by high proliferation and adoption of mobile communications. Speedy diffusion and adoption has exposed the Kenyan public to unprecedented individual security threats via the mobile platform. A national drive to foster awareness and nurture detection and coping skills is urgently required. This paper focuses on the role of governmental cybersecurity strategy in this area and explores the approaches to be used for improving public awareness of mobile Internet threats. Without addressing this vital aspect, the core aim of the strategy could be defeated, despite its comprehensiveness and excellence in other areas. This paper presents the outcome of an online study and comparative analysis of cybersecurity strategies of two developing countries. We conclude by proposing techniques for raising national awareness of cyber threats of mobile Internet, with a clear mandate to governments in developing countries to address this as a matter of urgency, and to include it in their respective cybersecurity strategies.

Keywords: Mobile Internet threats, mobile security threats, cybersecurity, awareness.

I. Background

Mobile phones have become ubiquitous and essential, especially in countries with underdeveloped landline infrastructures. In this paper we have focused on Kenya, a rapidly developing country. Kenya's mobile proliferation was profoundly influenced by her ICT revolution following the laying of undersea cables in 2009 that created high demand for the Internet.[1] The 2007 innovative mobile money transfer launched by Safaricom Kenya, a leading mobile network provider,[2] provided a platform for mobile network companies to embark on providing both data and voice services to citizens with increased Internet bandwidth.[3]

This has led to increased use and dependence on the Internet and has exposed the Kenyan public to unprecedented individual security threats. A number of cyber threats are perpetrated via the mobile Internet including mobile malware, identity theft, fraud, data theft.[4] Many of these attacks can be prevented either by using technology or by being wary and behaving more securely. Theoretically, if users were aware of how to protect themselves, the crimes could be prevented. Effective governmental strategies are thus urgently required to raise awareness in order to reduce cyber-attacks.[5] To address this, a number of governments have developed national cybersecurity strategies in response to increased cyber attacks against their critical infrastructures, economies and citizens.

Kenya has not, thus far, had a legislative framework in place to protect its mobile Internet users. Cybercrimes have gone unprosecuted since the diffusion of Internet usage and the aligned growth of cyber crime against Internet users.[6] This is against the backdrop of the provisions to fight cybercrime through the Kenya Information Communication Amendment Act 2009.[7] The problem is that Kenya's newly launched Cybersecurity Strategy, aimed at facilitating socio-economic growth through increased Internet usage is unclear on how government will address mobile Internet insecurity. This omission potentially undermines citizens' security. The strategy document is equally silent on the approaches the government will use to raise citizens' awareness of the cyber threats of mobile Internet. Von Solms and Von Solms acknowledge the failure by most African governments to provide any governmental support in attempting to raise the levels of cybersecurity amongst school children, which they note is becoming a growing problem.[8] Kenya, and other African nations, still lacks national cybersecurity awareness strategies.[9]

Studies have suggested that the human factor is the weakest link in the security of information systems, and public awareness and training are primary ways of improving this.[10] It is argued that the effectiveness of security solutions consisting of technolo-

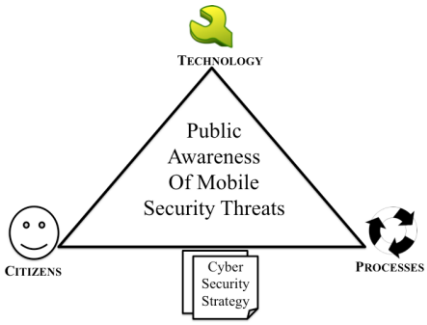

Figure 1. Conceptual framework.

gies, processes and people relies on people using the technologies securely and/or following the secure procedures[11] as depicted in Fig. 1 above. An effective security model requires the three elements to work effectively together. Citizens are a threat to security if they lack knowledge of security practices or are unable to properly apply such knowledge.[12] This emphasises the need to continuously raise public awareness on evolving Mobile Security Threats (MST) to improve citizen security (Section II). If the cybersecurity strategy does not specify how a significant sector of the public should be protected while using mobile Internet-enabled technology, it undermines the overall aim of the strategy to improve citizen security. We thus explored approaches the Kenyan government could and should use, via the new cybersecurity strategy, to improve awareness of MST, as a first step towards addressing the current deficiency in this area (Sections III, IV & V). We discuss our findings and reflect in Sections VI & VII. We conclude the paper in Section VII by proposing the use of a strategy that incorporates awareness drives reinforced by a robust legislative framework and government lead role to facilitate citizens' access to usable technology and information on MST.

II. Related Work

Cyber threats that used to target desktop computers have now migrated to a mobile ecosystem comprising of mobile devices, mobile sensors and mobile security devices.[13] Studies analysing mobile threats reveal that the growing uptake of smartphones—and their increasing connectivity and capability—resulted in a corresponding increase in attention from threat developers and security researchers.[14] For instance, in 2011 almost 64 % of mobile threats targeted the Android platform, as compared to iOS, BlackBerry and Windows.[15] The growth reached 94 % in 2012 and was attributed to the increasing demand for malicious tools and services that can be used to create and distribute mobile malware underground.[16] This resulted to growth of mobile malware and high-risk applications developed by malware authors that reached two million in the first quarter of 2014.[17]

The current usage of technical security mechanisms such as firewalls and intrusion prevention systems are inadequate in the face of risky mobile phone applications.[18] Certainly, as Android provides an open environment for both developers and users, coupled with its high market share of 79.3 % compared to iOS, Blackberry and Windows platforms, it is the primary focus of cybercriminals.[19] Android devices have proliferated Kenya's mobile market requiring the Communications Authority (CA) of Kenya to take action to deal with counterfeit phones.[20]

The richness of the data held on mobile devices makes them attractive to cyber criminals; they are capable of revealing useful data like geo-location, and are vulnerable to data loss and information leakage. This points to a developing threat of gathering in-

telligence on users' confidential information using mobile malware.[21] Moreover, criminals can manipulate the data without users' consent.[22] The development of mobile-specific malware is an increasing threat, mainly for Android and jail-broken iPhones[23] with various spyware, worms and root-exploits targeting the iPhone, most of which compromise the phone's content.[24] Studies have confirmed that mobile phones have been used as a platform for distributing viruses as well as a transmission of viruses over Bluetooth services.[25] In some instances, mobile phones have been used to propagate hate speech as evidenced in Kenya after the December 2007 elections that fuelled ethnic violence.[26] Similarly, in 2010, mobile Internet was used to disseminate mass propaganda that amplified the Arab Spring political uprisings in Egypt, Tunisia and Libya.[27]

Evidence pointing to an inherent worldwide MST mandates future studies to concentrate on MST landscape specifically in countries where the mobile platform has revolutionised the use of ICTs and is being used to conduct daily online activities without a concomitant level of awareness of such threats.

III. Study Design

We decided to conduct a survey in order to explore expert opinion about how public awareness of threats should be raised. A four-week cross-sectional online survey of key ICT stakeholders in Kenya published to a listserv, the Kenya ICT Action Network (KICTANet), was conducted. KICTANet is a multi-stakeholder ICT policy discussion forum comprised of 758 members representing 38 ICT stakeholder groups from the civil society, public and private sectors, academia, development partners and media.[28] Its mandate is to speed up ICT policy development in Kenya.

The Survey Monkey tool was used to develop and administer questionnaires and collect responses. The completed questionnaires were stored in Survey Monkey's database, which the researcher retrieved for analysis. The Survey Monkey tool has an analysis feature which the researcher used to statistically analyse the demographic data. The NVivo tool was used to code and analyse the textual data through themes that were identified. The survey responses were stratified into six strata representing each stakeholder group. As it was not possible to determine the distribution of members in each stakeholder strata that make up KICTANet's 758 total membership, six sets of different numbers randomly generated by Research Randomizer were used to represent the sample that was analysed to ensure there was an equal chance of every response to be chosen and represented in the sample.

In addition to the survey, comparative analyses were conducted on South Africa and Kenya's MST landscape and the approaches used by both nations to create threat

awareness delivered an in-depth examination of approaches the Kenyan government ought to adopt to raise public awareness of MST.

IV. Comparative Analyses

A. Kenya vs South Africa

South Africa, as the only African nation to have published its cybersecurity policy, provides a good benchmark for comparison to Kenya regarding cybersecurity awareness and MST. The two nations have had similar ICT revolutions and mobile proliferation where mobile network companies provide both data and voice services to citizens with increased Internet bandwidth.[29] In fact, South Africa has been used as a benchmark by the OECD in mobile proliferation studies[30] although IDG Connect reports that its Internet penetration remains low at only 14 % due to poor information infrastructure.[31] Nevertheless, compared with other polled African nations in a study investigating Internet usage, Kenya and South Africa reported high mobile Internet usage of 77.8% and 70% respectively across other devices.[32] Moreover, 63 % of Kenyans and South Africans stated in another study that mobile Internet has greatly improved their lives.[33]

Kenya ranks fourth in Africa with 21 million Internet users as compared to South Africa's 24 million Internet users against a population of 45 million and 48 million respectively.[34] However, with the growing Internet penetration, users in Africa are not security aware due to lack of knowledge, understanding, expertise and awareness, exacerbating the cybercrime predicament in developing countries.[35] Specifically for Kenya, IDG Connect affirms that cybercrime poses the greatest challenge to the police and organisations, costing Kenya $36 million per year.[36]

Instructively, Serianu's 2012 Kenya Cybersecurity Report indicates that the threat to mobile phone users has increased with malware authors re-inventing existing malware for mobile devices and also creating mobile-specific malware targeted to distinctive mobile opportunities such as mobile banking.[37] Mobile money fraud, phishing and mobile banking malware are among threats that target individuals, organisations and critical infrastructure.[38] Kenya ranked 70th in the world and 10th in Africa for malicious code, while for hosting phishing websites she is ranked 5th in Africa.[39]

Meanwhile in South Africa, the propagation of malware through mobile devices, social networks and web navigation has increased the rate of cybercrime following the increased use of mobile phones.[40] The use of social networks and mobile devices plays a significant role in aiding Internet related fraud through mobile malware.[41] SIM cloning, where cyber criminals attempt to intercept communications between an online bank and the target are on the increase.[42] Identity theft is also an increasing threat in the mobile platform where abuse of identity forms the basis of occupational

fraud and cybercrime.[43] Finally, there is a huge shortage of skilled resources for the development of secure applications with even non-malicious applications being developed without security features, meaning they can also be compromised.[44] Comparatively speaking, there is a gap in documenting MST in Kenya to inform awareness initiatives and security policy making, unlike South Africa.

B. Awareness Approaches in South Africa

Calls to the South African government to initiate continuous cybersecurity awareness all year round and the department of education to include it in the education curriculum were heeded by Reid and Van Niekerk's annual education campaigns since 2011 with the aim to educate South Africa's youth about cyber issues.[45] Topics such as online activities, cybercrime, social networking, password and hardware security, malware, cyber bullying, cyber identity management among others are covered through the campaign's education.[46] A voluntary hand-crafted or digitally-created poster contest follows thereafter to measure the campaign's impact on the involved youth's awareness levels on the covered security issues.[47] The campaigns have reported improved youth participation, cybersecurity awareness and inclusion of teachers who positively impacted the study. An interdisciplinary approach where cybersecurity experts determine what users are taught, with other experts such as teachers crafting the message is recommended.[48]

Meanwhile, in an attempt to empower African school teachers to educate children on cybersecurity, Von Solms and Von Solms created a video-based syllabus to teach children how to protect themselves when exploring the Internet subsequently nurturing development of a cybersecurity culture.[49] Utilisation of open education resources on cyber topics to empower teachers to educate children on using cyberspace safely is proposed.[50] Through a search of e-safety children videos on YouTube, the authors liaised with teachers to analyse the most suitable videos and made three distinct video-based cybersecurity syllabuses for African children in three different age groups between ages 7 and 13.[51] Clearly, the approach highlights the importance of developing a national cybersecurity culture and involving teachers in creating awareness amongst the youth, which will ensure that the next generation are well prepared for the evolving threat landscape.

Additionally, privately run initiatives such as *Cellphone Safety* managed by independent non-commercial institutions and Cybercrime.co.za that serve as an awareness portal aimed at educating individuals on criminal exploitation of ICTs in South Africa and the rest of Africa[52] support cybersecurity awareness initiatives in South Africa. Similarly, scholars indicate that there a number of cybersecurity awareness programs aimed at educating users in different geographical parts of South Africa are necessitated by increased rate of bandwidth consumption in the country.[53] Research studies

that have been conducted in parts of South Africa have indicated an increased level of awareness and citizen online behaviour.[54]

C. Analysis of Kenya's MST landscape

It was instructive to launch the study by gathering knowledge about prevalent threats related to mobile Internet platforms where the identified themes confirmed the MST analyses reviewed in the literature. The technical threats including malware attacks, identity theft, phishing, botnet attacks, mobile banking fraud, malicious third-party applications, were posited as growing MST by Symantec Internet Security Threat Report, McAfee Lab Threat Report, ENISA top ten mobile threats, NIST, F-Secure Lab Report, and Serianu 2014 Kenya Cybersecurity Report. Equally so, the non-technical threats, including low IT literacy, data breaches, legal loopholes, limited police capacity to fight cybercrime, were highlighted by other research[55] as being prevalent in Kenya.

Evidently, Kenya's MST analysis confirms ENISA and Symantec's reports that computer threats have moved to the mobile platform. It also confirms that these studies can be usefully employed to extend our understanding of Kenya's MST landscape. The analysis should therefore be useful to government when designing approaches to improving public awareness on threat detection and coping skills.

D. Current Kenyan Approach

1) Kenya's ICTA's Awareness Initiative

This study recognises the recent partnership formed between ICTA and the University of Nairobi's C4DLab in offering quarterly training to IT professionals in government and private sector to develop experts who will understand and counter cyber threats, and prepare cyber strategies for their organisations.[56] However, since the training targets primarily IT professionals at a cost of Kenyan shillings 50,000 (£335) for each self-sponsoring participant, it falls short in fostering a comprehensive public awareness required of MST. A national awareness program targeting all sectors of society would have more impact.

2) Role of KE-CIRT/CC on Mobile Internet Security

CAK is mandated by the Kenya Communications Act of 1998 to establish a national cybersecurity management framework that creates the National Kenya Computer Incident Response Team Coordination Centre 1 (KE-CIRT) to coordinate response and manage cybersecurity incidents nationally.[57] Aside from acting as Kenya's national cybersecurity trusted point of contact for information security matters, KE-CIRT/CC is mandated to create and maintain awareness on cybersecurity-related activities.

Certainly, compared to South Africa, which has not yet established its national CERT (or CIRT) but has national awareness campaigns on cybersecurity,[58] the Kenyan public needs awareness on the roles of the national KE-CIRT/CC in mitigating cyber threats and specifically MST. The prediction is that if the government does not create comprehensive national awareness drives targeting all sectors of society on the evolving MST, it undermines the overall aim of the cybersecurity strategy to improve citizens' security, neither will it deal with human factor in the security chain.

V. Findings

A. Response Rate

There were 58 responses that were categorised into six strata. Five responses could not be grouped into any strata as the respondents skipped the question requiring them to indicate the sector they belonged to. Since they could not be grouped in any stratum, they were added to the unusable questionnaires totalling to 8 responses. There were more male respondents than female who fell in the age bracket of 30-39 with the highest participation coming from the public sector strata. Participants with postgraduate education level had more access to the strategy document than those with graduate, high school and tertiary college education. This suggests that Kenya's public access to documents is determined by level of education.

The comparative analyses of Kenya and South Africa's MST confirmed the prevalence of both technical and nontechnical MST in these countries. This suggests the need for documenting MST in countries that have vibrant mobile Internet societies to inform awareness drives and Cybersecurity strategies. Indeed, the awareness approaches used in South Africa cut across various sectors of society using mobile In-

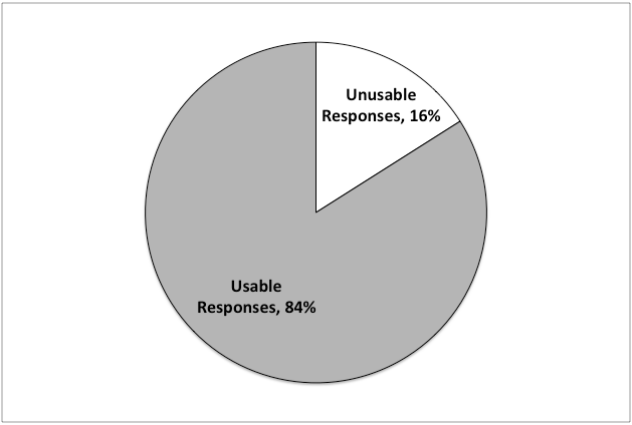

Figure 2. Response classification.

ternet unlike Kenya, requiring the need for the Kenyan government to roll out national awareness drives on MST.

B. MST in Kenya

MST data analysis identified two themes in the type of threats riddling mobile security; technical and nontechnical. Technical threats, which are the most commonly experienced, rated at 57% included malware attacks, hacking, mobile banking fraud, adware, spam, phishing, identity theft, fake third-party applications, cybercrime, botnet attacks, cyber espionage and insider threats. The non-technical threats, rated at 43%, included use of mobile Internet to spread hate messages, cyber bullying, negligence of mobile network providers to register Internet subscribers, limited capacity of police force to combat cybercrime, terrorism threats, inadequate legislation to fight cybercrime and hackers, infringement of privacy, low IT literacy, social engineering attacks, social network attacks and personal data breaches.

Further analysis of the two themes revealed evidence of a lack of public awareness on how to detect and avert both technical and non-technical MST. This undeniably amplifies their success rate. There was also a suggestion that the public is unaware of how to protect itself while using their smartphones.

C. Approaches to address MST

In exploring the research question on how the government envisages to address both technical and non-technical MST, three main themes were identified: public awareness drives rated at 63%, technology at 21% and law enforcement at 16% of the total responses. These themes are discussed further in the next subsections.

1) Awareness Drives

The proponents of public awareness drives, particularly from the private sector, media and academia, posited that empowering people with knowledge and basic skills such as password design and social networking safety practices would support users in improving mobile security. There is a clear perception of a lack of understanding and knowledge related to precautions to be taken. The respondents felt that the public lacked understanding of the dangers of insecure practices such as downloading third-party applications, logging onto dangerous sites and releasing personal information to social engineering sites.

Proposals for Awareness Drives. Responses to the questions that sought participants' thoughts on public awareness drives the government should use to sensitise citizens to MST identified four themes:

(1) Media campaigns through the use of print, electronic and social media networks were the most preferred awareness drives at 52% of the responses;

(2) Public forums such as community gatherings, public conferences, road shows and use of Provincial Administration rated at 24%;

(3) The introduction of Cybersecurity lessons in the education curriculum rated at 13%;

(4) A text alerts system where mobile network providers would send information on threats to their subscribers was suggested as awareness drives rating at 11%.

Government Support. Submissions on programs the government should develop to support the public in adapting to the evolving nature of MST, reporting MST and accessing information on MST included training and education rating at 51%, information portal at 27% and help desks at 22% of the responses.

2) Technology Training

The use of technical measures to address MST was accompanied by calls for government to invest in technology that would support public awareness programs. Specifically, civil society and private sector proposed that government should protect the information infrastructure via technical means to ensure that Kenya's cyber space is reasonably secure to enable secure communication and business transactions. They further referred to the need for government to engage mobile network providers when implementing tailored technologies to protect mobile users without infringing on their privacy rights. However, the public sector countered that technology alone would neither increase awareness, nor reduce MST if there is poor public IT knowledge of the actual technology on the devices. They suggested the need for public education and training on securing the technology.

3) Law Enforcement

The third theme, using law enforcement, was proposed by all participants as a way to reinforce public awareness initiatives to address MST. The participants argued that the public lacked awareness not only of measures to protect itself from MST but also on the laws intended to counter the threats. The private sector participants proposed the need for government initiatives to educate both the public and police on laws on cybercrime and consequences of violating extant laws on cybercrime, mobile money fraud and spreading of hate speech using mobile Internet. The three themes clearly delineate the requirement of an interwoven yet tailored approach that addresses different societal needs on MST.

VI. Discussion

1) Approaches to Deploy in Kenya

A focus on improving public awareness was the most favoured approach. Participants proposed empowering citizens with knowledge and basic cybersecurity skills in a bid to improve MST detection and coping skills. While one of KE-CIRT/CC's roles is cybersecurity awareness creation and maintenance, the results indicate that the majority of the public are unaware of this role. This strengthens the study's findings on public awareness and makes publication of KE-CIRT/CC's cybersecurity awareness mandate critical.

Additionally, the ICTA and C4DLab's partnership on cybersecurity training, albeit targeting only a specific sector,[59] reinforces the public awareness theme as revealed by the comparative analysis on approaches used in Kenya. While it is a useful initiative, it excludes an important segment of Kenya's population, the youth, while RIA's statistics indicate that 77.8% mobile Internet users started doing so at the age of 15.[60] To underscore the importance of targeting all citizens including youth, the study reflects on the positive impact achieved by cybersecurity awareness approaches employed in South Africa targeting the youth from primary schools.[61]

2) Awareness drives to raise prominence of MST

In exploring the research question on whether the Kenyan government considered using public awareness drives on cyber threats when using mobile Internet, it was important for the study to acknowledge the awareness efforts already underway with ICTA and C4DLab in the lead.[62] As the training is the first of its kind in Kenya, this study's findings argue for the requirement of government to roll out more awareness campaigns targeting all sectors of society using mobile Internet.

Four main themes emerged which have implications for the investigation of awareness initiatives the government should deploy. The media campaigns theme was favoured by the majority of participants who suggested using print, electronic and social media networks to publicise MST, as supported by ITU's public campaigns.[63]

Certainly, the themes of public forums and engagement with mobile network providers are reinforced by ITU's advocacy for public-private partnerships in creating awareness to fight cyber threats.[64] It is conscionable for participants to require the government to take the lead role in ensuring that mobile network providers take responsibility in protecting Internet subscribers as they control the largest Internet market share in Kenya.

The introduction of cybersecurity lessons in schools was evidenced in the survey results and also supported by the comparative analysis of South Africa's awareness drives by Reid and Van Niekerk's annual education campaign and Von Solms and

Von Solms' video-based syllabus for primary schools.[65] ITU also recommends the introduction of cyber threats lessons in schools and universities.[66] This confirms that—so far as the requirement to develop a cybersecurity awareness culture in society is concerned—it is prudent to begin with the youth who are increasingly using mobile Internet.

The four themes confirm that despite the Kenyan government having only just begun quarterly awareness drives in one sector, there is a need for sustained awareness drives targeting different sectors of society using mobile Internet.

3) Role of Government in Supporting Citizens

a) Through Cybersecurity Strategy

The findings indicate that the themes of information portals and help desks can be useful in extending our understanding of the role of KE-CIRT/CC and dedicated toll free lines at the Criminal Investigations Department (CID) to help the public report cyber incidents and access threat information. Geer advocates for mandatory reporting of cyber incidents based on thresholds set by law.[67] Wolf Pack's 2013 security report on South Africa that proposed establishment of a national and sector CSIRTs to coordinate incidence reporting and response to threats also supports these findings.[68]

The information portal theme also suggested conducting surveys on threat awareness and prevalence, and publishing results that are publically accessible via CAK's website. Upon reviewing KE-CIRT/CC's functions, the study found out that it is mandated to carry out research on computer threats, and now – on MST, and to publish results. Indeed, ITU proposes the collection and publication of relevant information to determine threat levels as a way to informing users. Articles and newsletters about security are one way of spreading awareness[69] as evidenced from the comparative analysis results of South Africa's Cybercrime.co.za awareness portal on cybersecurity issues and Cellphone Safety program on children's mobiles.[70] Equally so, Von Solms and Von Solms' acknowledgement of most African governments' failure to provide support to attempts to raise the levels of cybersecurity[71] backs the requirement of government support to citizens in managing MST.

b) Training

The survey results and comparative analysis on awareness approaches underscore the impact of including cybersecurity lessons in schools to inform the youth on the latest cyber threats and how to protect themselves. Strong support for technical means to dealing with MST was clearly evident in the results. In fact Schneier argues for the design of better security systems that assume uneducated users and prevent them from changing security settings in a way exposing them to risks.[72] However, research on security awareness recommends for effective training for users to operate securely

since a purely technical approach is insufficient.[73] Cybersecurity training conducted by Reid and Van Niekerk among South Africa's youth supports the requirement of including cyber topics in curriculum and improving awareness on MST. Essentially, this confirms that user awareness and education on MST is important in efforts to improve citizens' security.

c) Changes to Kenyan Law

The themes of technology and law enforcement were also identified as ways to reinforce public awareness drives and coping skills of MST. Serianu's 2012 Report on Kenya's Cybersecurity highlighted Kenya's legal gap in cybersecurity where cybercrimes go unprosecuted and leave the victims vulnerable.[74] Law enforcement is also supported by Magutu et al.'s 2011 study on mitigations of cybercrime underpinning the gap left by lack of proper cyber-legislation to prosecute cybercrimes including spamming, phishing, malware and hacking,[75] as well as curb incidences of using mobile communications to spread hate speech in Kenya.[76] Botnet attacks in Kenya and legal loopholes certainly confirm Christin et al.'s 2011 study that explored the perspective of botnet operators who associate risks of hosting bot operations in countries with ambiguous or non-existent cybercrime laws.[77] The results of the current study endorse the law and the importance of public awareness as a deterrent for perpetrating mobile Internet crimes.

4) Summary

Overall, the study's findings confirm the importance of public awareness on MST to help improve citizens' security. The cybersecurity strategy ought to incorporate the law, facilitate citizens' access to usable technology, processes and information on MST. These would inform tailored awareness drives targeting all sectors of society using mobile Internet, provide security assessments, training programs and constitute government's role on reducing MST. Hence, we propose an improved conceptual framework that incorporates the suggestions from the findings and literature review, as shown in Figure 3, to help create public awareness of MST.

VII. Reflection

The study aimed to investigate approaches the Kenyan government should use to improve citizens' awareness on MST through the cybersecurity strategy. Projected growth of Kenya's mobile Internet requires awareness drives that will improve cyber threat detection and coping skills of different sectors of society using mobile Internet. The findings have confirmed the importance of considering the concept of human factor in the security link by delineating the requirement of public awareness on MST to improve citizen's security.

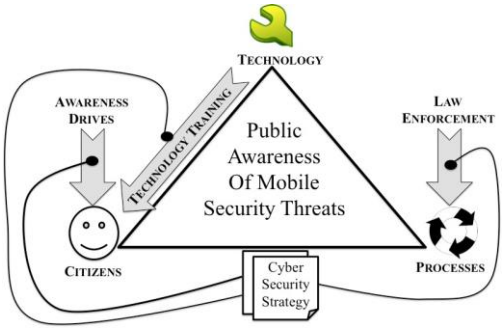

Figure 3. Proposed Conceptual Framework.

1) Implications of Findings

Applying a two-pronged approach proved beneficial to the main contributions of this research because the researchers were able to use comparative analyses on South Africa and Kenya's MST and awareness approaches, as well as survey data, to answer the research questions. The main contribution of this research is the demonstration of the requirement for awareness drives to be sustained in all sectors of society to improve mobile Internet security in Kenya. The study suggests that awareness drives would be strengthened by widespread, easily accessible technology and a good legal framework.

On the basis of the MST analyses, the findings of MST prevalent in Kenya can be a useful springboard for designing awareness drives that the government may deploy to meet varying technical levels of society. Evidence also requires the government's lead role to support the public adaptation to the evolving nature of MST through e-government.

The findings lead to the conclusion that countries with vibrant mobile Internet societies must act to improve the cybersecurity awareness of their mobile Internet users within the context of secure technology and robust legal framework or stringent cybercrime laws. Consequently, the development of cybersecurity strategies that endorse public awareness campaigns of MST exemplifies the integral component and role of cybersecurity strategies to citizens' security as evidenced in this study.

2) Proposed Recommendations

Creating MST awareness for all societal sectors is not easy in a society with disparate IT skills. However, it is incumbent on government as a key stakeholder in security to take the lead role in the campaign. The study has devised some recommendations to support the government's role:

- Tailor specific awareness programs: to support the ICTA's cybersecurity professional training, specific and measurable awareness programs must target different technical levels of all sectors of society and their impact evaluated.[78]
- Information portals: availability of, and access to threat information on CAK, CID, KE-CIRT/CC websites and Huduma Centers would spread awareness and provide support to the public in more decentralized ways helping them adapt to the evolving MST. Use of awareness tools through different media and public campaigns are successful ways of spreading awareness to reach audiences of different technical levels.[79]
- Surveys: national surveys on cybersecurity awareness, usable and reasonably secure mobile technology drawing participants from different sectors of society would be useful in identifying gaps and trends which can inform awareness programs. ITU recommends the collection and publication of relevant information to determine threat levels as a way to inform users,[80] and surveys are a way to achieve this.
- Government regulation: mobile network providers' use of insecure mobile technologies rendering users vulnerable to MST should be met with serious government penalties. Herley et al. advocate for more government regulation to address the difference in power that allows service providers to shift losses to users when security breaches occur.[81]

3) Limitations of the Study

The research used web-based survey to collect data from key stakeholders of ICT in Kenya. The main limitation faced was the lack of direct access to the respondents to ask further questions as they could only be reached through the listserv. There was also time constraint to collect the data and learn different features of NVivo that was used to code and thematically analyse the textual data. Key challenges faced were the difficulty in accessing vital information, especially from government sources without due authorization and cost of paying for the online tools.

VIII. Conclusions and Future Work

It is proposed that future research in this area be carried out to specifically measure the effectiveness of cybersecurity awareness approaches in countries with vibrant mobile Internet societies that have implemented awareness drives. This would set a benchmark for those developing or yet to develop their cybersecurity strategies. Additionally, more research concentrating on MST landscape in countries with vibrant mobile Internet societies would be useful as this study confirms that these threats are on the rise in Kenya, and the same may be happening elsewhere.

Acknowledgement

The undertaken research was granted ethical approval by the College for Social Sciences ethical committee at our University.

Notes:

[1] David Souter and Monica Kerrets-Makau, "Internet Governance in Kenya: An Assessment," ICT Development Associates Ltd, 2012, available at www.internetsociety.org/sites/default/files/ISOC%20study%20of%20IG%20in%20Kenya%20-%20D%20Souter%20%26%20M%20Kerretts-Makau%20-%20final.pdf; Gabriel Demombynes and Aaron Thegeya, "Kenya's Mobile Revolution and the Promise of Mobile Savings," *Poverty Reduction and Economic Management Unit, Africa Region World Bank, 2012*, available at http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-5988.

[2] Demombynes and Thegeya, "Kenya's Mobile Revolution and the Promise of Mobile Savings."

[3] IDG Connect, "Africa 2013, Cybercrime, Hacking and Malware," 2013, available at www.idgconnect.com/download/11401/africa-2013-cyber-crime-hacking-malware?source=connect.; Enrico Calandro, Cristoph Stork, and Alison Gillwald, "Internet Going Mobile: Internet Access and Usage in 11 African Countries," *Research ICT Africa*, 2012, available at http://www.researchictafrica.net/publications/Country_Specific_Policy_Briefs/Internet_going_mobile_-_Internet_access_and_usage_in_11_African_countries.pdf.; CAK, "Internet Market Analysis Study," 2007 available at http://www.ca.go.ke/images/downloads/RESEARCH/Internet%20Market%20Analysis%20Study%20Final%20Report.pdf.

[4] Serianu Ltd., "Kenya Cybersecurity Report 2014. Rethinking cyber security "An Integrated Approach: Process, Intelligence and Monitoring," 2014, available at http://www.cyberusalama.co.ke/reports/2014/Kenya%20Cyber%20Security%20Report%202014.pdf.

[5] ITU, "Understanding Cybercrime: A guide for developing countries" (ITU Telecommunication Development Centre, 2009), available from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

[6] Serianu Ltd., "Kenya Cybersecurity Report 2014. Rethinking cyber security "An Integrated Approach: Process, Intelligence and Monitoring."

[7] ICT Authority, "Kenya's ICT Master Plan 2014-2017," 2013, available at www.icta.go.ke/national-ict-masterplan/.

[8] Suné Von Solms, and Roussouw Von Solms, "Towards Cyber Safety Education in Primary Schools in Africa," HAISA, 2014 available at www.cscan.org/default.asp?page=openaccess&eid=15&id=247.

[9] Ibid.

[10] F.P. Bresz, "People – Often the Weakest Link in Security, but One of the Best Places to Start," *Journal of Healthcare Compliance* 6, no. 4 (2004): 57-60; Rayne Reid and Johan Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture," Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), 174-184, available at www.cscan.org/default.asp?page=openaccess&eid=15&id=249.

[11] Reid and Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture."

[12] Ibid.

[13] ENISA, "ENISA threat Landscape 2013 – Overview of Current and Emerging Cyber Threats," 2013, available at www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport.

[14] ITU, "Understanding Cybercrime: A guide for developing countries"; Symantec, "Internet Security Threat Report," 2014, available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_ 21291018.en-us.pdf; Kaspersky, "The Threat Landscape," 2014, available at http://media.kaspersky.com/en/business-security/kaspersky-threat-landscape-it-online- security-guide.pdf.

[15] Kaspersky, "The Threat Landscape."

[16] ITU, "Understanding Cybercrime: A guide for developing countries;"; Symantec, "Internet Security Threat Report;" Kaspersky, "The Threat Landscape."

[17] ITU, "Understanding Cybercrime: A guide for developing countries."

[18] Caleb Barlow, "Highlights and Insights," RSA 2014 Conference, 2014, available at http://ddos.inforisktoday.com/interviews/how-mobile-hacks-threaten-enterprise-i-2199; NIST, "The role of NIST and Technology in Mobile Security," 2014, available at http://csrc.nist.gov/documents/nist-mobile-security-report.pdf.

[19] ITU, "Understanding Cybercrime: A guide for developing countries;" Symantec, "Internet Security Threat Report;" Kaspersky, "The Threat Landscape;" F-Secure Lab, "Mobile Threat Report," 2013, available at www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf; McAfee, "McAfee Lab Threat Report: Third Quarter 2013," 2013, available at http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf.

[20] Macharia Kamau, "Kenya Wants EAC States to Hasten Fake Phone Switch Off," Standard Digital, 28 June 2013, http://www.standardmedia.co.ke/business/article/2000086969/kenya-wants-eac-states-to-hasten-fake-phone-switch-off 7/07/2013; Winfred Kigwe, "Kenya: 1.9 million Fake Phones Shut," All Africa, 2 October 2012, available at http://allafrica.com/stories/201210020512.html.

[21] Brett van Niekerk and Manoj Maharaj, "Mobile Security from an Information Warfare Perspective," Information Security for South Africa (ISSA), 2010, available at http://dx.doi.org/10.1109/ISSA.2010.5588339; Nicolas Seriot, "iPhone Privacy," Black Hat DC 2010, available at www.blackhat.com/presentations/bh-dc-10/Seriot_Nicolas/BlackHat-DC-2010-Seriot-iPhone-Privacy-slides.pdf.

[22] Karen Renaud, and Wendy Goucher, "Monkey See – Money Take Photo: The Risk of Mobile Information Leakage," *International Journal of Cyber Warfare and Terrorism* 3, no. 4 (2013), http://dx.doi.org/10.4018/ijcwt.2013100105; ENISA, "ENISA threat Landscape 2013 – Overview of Current and Emerging Cyber Threats."

[23] Bill Morrow, "BYOD Security challenges: control and protect your most sensitive data," *Network Security* 12 (2012): 5-8, http://dx.doi.org/10.1016/S1353-4858(12)70111-3.

[24] Nicolas Seriot, "iPhone Privacy."

[25] Van Niekerk and Maharaj, "Mobile Security from an Information Warfare Perspective"; Nicolas Seriot, "iPhone Privacy."

[26] Alexis Okeowo, "SMSs used as a tool of hate in Kenya," *The Mail and Guardian*, 19 February 2008, available at http://mg.co.za/article/2008-02-19-smss-used-as-a-tool-of-hate-in-kenya.

[27] Philip Howard and Muzammil Hussain, *Democracy Fourth Wave? Digital Media and the Arab Spring* (Oxford: Oxford University Press, 2013).

[28] KICTANet, "KICTANet 28-29 September 2007 Workshop Report," 2007, available at http://www.kictanet.or.ke/documents/instassessment/KICTANet-28-29-September-2007-Workshop-Report.pdf.

[29] IDG Connect, "Africa 2013, Cybercrime, Hacking and Malware"; Calandro, Stork, and Gillwald, "Internet Going Mobile: Internet Access and Usage in 11 African Countries"; CAK, "Internet Market Analysis Study."

[30] Calandro, Stork, and Gillwald, "Internet Going Mobile: Internet Access and Usage in 11 African Countries"; CAK, "Internet Market Analysis Study."

[31] IDG Connect, "Africa 2013, Cybercrime, Hacking and Malware."

[32] Calandro, Stork, and Gillwald, "Internet Going Mobile: Internet Access and Usage in 11 African Countries."

[33] On Device Research, "Impact of mobile Internet on people in Kenya, Nigeria and South Africa," 2014, available at https://ondeviceresearch.com/blog/mobile-internet-kenya-nigeria-south-africa-2014.

[34] World Internet Statistics, "Internet Usage Statistics for Africa," 2014, available at http://www.internetworldstats.com/stats1.htm.

[35] WolfPack, "The South African Cyber Threat Barometer," 2012/3, available at http://www.bic-trust.eu/files/2012/10/SA-2012-Cyber-Threat-Barometer_Medium_res.pdf.

[36] IDG Connect, "Africa 2013, Cybercrime, Hacking and Malware."

[37] Serianu Ltd., Kenya Cybersecurity Report 2014. Rethinking cyber security: "An Integrated Approach: Process, Intelligence and Monitoring."

[38] Symantec, "Internet Security Threat Report;" Serianu Ltd., "Kenya Cyber Security Report," 2012, available at www.serianu.com/downloads/KenyaCyberSecurityReport2012.pdf.

[39] Serianu Ltd., "Kenya Cyber Security Report," 2012.

[40] WolfPack, "The South African Cyber Threat Barometer," 2012/3.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Reid and Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture."

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Von Solms and Von Solms, "Towards Cyber Safety Education in Primary Schools in Africa."

[50] Ibid.

[51] Ibid.

[52] Cellphone Safety website, http://www.cellphonesafety.co.za; Cybercrime, "Local Resources on Cybercrime," http://cybercrime.org.za/local-resources.

[53] Martie Grobler, Joey Jansen Van Vuuren, and Louise Leenen, "Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward," Council for Scientific and Industrial Research, 2012, available at http://krr.meraka.org.za/~lleenen/Grobler_Final.pdf.

[54] Grobler, Jansen, Van Vuuren, and Leenen, "Implementation of a Cyber Security Policy in South Africa."

[55] IDG Connect, "Africa 2013, Cybercrime, Hacking and Malware"; Serianu, "Kenya Cybersecurity Report 2014"; Peterson Obara Magutu, Gladys Monchari Ondimu and Christopher Jilo Ipu, "Effects of Cybercrime on State Security: Types, Impact and Mitigations with Fibre Optic Deployment in Kenya," *Journal of Information Assurance & Cybersecurity* (2011), http://dx.doi.org/10.2011.618585.

[56] ICT Authority, "Kenya's ICT Master Plan 2014-2017;" ICT Authority and C4DLab, "Cybersecurity Training," 2014, available at http://www.c4dlab.ac.ke/training/cybersecurity.

[57] CAK, "Internet Market Analysis Study."

[58] Reid and Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture"; WolfPack, "The South African Cyber Threat Barometer"; Grobler, Jansen, Van Vuuren, and Leenen, "Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward."

[59] ICT Authority and C4DLab, "Cybersecurity Training."

[60] Calandro, Stork, and Gillwald, "Internet Going Mobile: Internet Access and Usage in 11 African Countries."

[61] Reid and Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture"; Von Solms and Von Solms, "Towards Cyber Safety Education in Primary Schools in Africa."

[62] ICT Authority and C4DLab, "Cybersecurity Training."

[63] ITU, "Understanding Cybercrime: A guide for developing countries."

[64] Ibid.

[65] Reid and Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture"; Von Solms and Von Solms, "Towards Cyber Safety Education in Primary Schools in Africa."

[66] ITU, "Understanding Cybercrime: A guide for developing countries."

[67] Dan Geer, "Cybersecurity as Realpolitik", Black Hat USA 2014 Conference, available at https://www.youtube.com/watch?v=nT-TGvYOBpI.

[68] WolfPack, "The South African Cyber Threat Barometer."

[69] Cormac Herley, P.C. van Oorschot, and Andrew Patrick, "Passwords: If We're So Smart, Why Are We Still Using Them?" in *Financial Cryptography and Data Security* (Berlin/Heidelberg: Springer, 2009), 230-237, available at http://dx.doi.org/10.1007/978-3-642-03549-4_14.

[70] Cellphone Safety website, http://www.cellphonesafety.co.za; Cybercrime, "Local Resources on Cybercrime," http://cybercrime.org.za/local-resources.

[71] Von Solms and Von Solms, "Towards Cyber Safety Education in Primary Schools in Africa."

[72] Bruce Schneier, *Carry On: Sound Advice from Schneier on Security* (Indianapolis, IN: John Wiley, 2014); Jackie Phahlamohlaka, Joey Jansen Van Vuuren, and A. C. Coetzee, "Cyber Security Awareness Toolkit for National Security: An Approach to South Africa's Cyber Security Policy Implementation," 2011, available at http://researchspace.csir.co.za/dspace/bitstream/10204/5162/1/Phahlamohlaka_2011.pdf.

[73] Renaud and Goucher, "Monkey See – Money Take Photo"; Phahlamohlaka, Van Vuuren, and Coetzee, "Cyber Security Awareness Toolkit for National Security."

[74] Serianu, "Kenya Cyber Security Report," 2012.

[75] Magutu, Ondimu and Ipu, "Effects of Cybercrime on State Security."

[76] Alexis Okeowo, "SMSs used as a tool of hate in Kenya."

[77] Nicholas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags, "It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice," in in *Financial Cryptography and Data Security* (Berlin/ Heidelberg: Springer, 2012), 16-30, available at http://dx.doi.org/10.1007/978-3-642-27576-0_2.

[78] Reid and Van Niekerk, "Towards an Education Campaign for Fostering a Societal Cyber Security Culture."

[79] ITU, "Understanding Cybercrime: A guide for developing countries," 30, 38; Enterprise Risk Management, "Social Engineering: People Hacking", in *Control Essentials* (2009), available at www.emrisk.com/sites/default/files/newsletters/ERMNewsletter_november_2009.pdf.

[80] ITU, "Understanding Cybercrime: A guide for developing countries."

[81] Herley, Van Oorschot, and Patrick, "Passwords: If We're So Smart, Why Are We Still Using Them?"

Angela OKUKU did this work while she was a Masters student, funded by a British Government Chevening Scholarships Award. She now works as a National Counter Terrorism Centre: Information Security Analyst.

Karen RENAUD's research focuses on human-centred security, a branch of Human Computer Inter-action (HCI). She is interested in the interplay between users and security in the context of societal and industrial use. She wants to work towards creating a natural easy, yet secure, interaction between humans, systems and devices. Her work has a strong development, experimental and deployment focus, testing solutions in practical situations. She has come up with a number of novel solutions to improve usability in a wide range of situations. Corresponding Author: karen.renaud@glasgow.ac.uk.

Brandon VALERIANO is a Senior Lecturer at the University of Glasgow in the School of Social and Political Sciences (also in the area of Global Security). Dr. Valeriano's main research interests include investigations of the causes of conflict and peace in the international system, as well as the study race/ethnicity from the international perspective. Ongoing and past research explores interstate rivalry, classification systems of war, the causes and consequences of military spending dynamics, cyber conflict, popular culture and foreign policy, and Latino foreign policy issues.