"I Am Because We Are": Developing and Nurturing an African Digital Security Culture

Karen Renaud[1], Stephen Flowerday[2], Lotfi ben Othmane[3], Melanie Volkamer[4,5]

[1]University of Glasgow, [2]University of Fort Hare, [3]Fraunhofer Institute for Secure Information Technology, [4]Technische Universität Darmstadt, [5]Karlstad University
karen.renaud@glasgow.ac.uk; sflowerday@ufh.ac.za; lotfiben.othmane@cased.de; melanie.volkamer@cased.de

Abstract

Technical solutions fail if people experience difficulties using them. Sometimes these difficulties force people to work around the security solutions in order to achieve legitimate goals. Improving usability undoubtedly helps, but this has not improved the situation as much as anticipated. In this paper we consider a variety of other reasons for non-uptake.

We argue that this situation can only be addressed by considering the person as a member of the wider community and not as a solitary agent. This aligns with the traditional African wisdom of *Ubuntu*: "I am because we are". We propose improving the *African Digital Security Culture* (ADSC): collective knowledge, common practices, and intuitive common security and privacy behaviour, in a particular society. We suggest a set of approaches for developing and sustaining ADSC in a society, for as members of a society we learn most effectively from each other, not from books, the media or by carrying out searches using search engines.

Keywords

Society; Information Security; Ubuntu

1. Introduction

The African philosophy of *Ubuntu* is considered to reflect the belief in a universal bond of sharing that connects all humanity. Nafukho (2006) explains that '*in traditional African society adult learning was viewed as holistic learning for life and work and formed the foundation of many African societies*' (p. 408). He explains that this has lapsed somewhat, meaning that adult learning is not supported as much as it used to be, under the Ubuntu paradigm. In this paper we will argue that a resurgence of the Ubuntu mindset presents us with an opportunity to improve African resilience to online threats.

Sub-Saharan Africa has experienced a growth in mobile telephony that dwarfs the developed world. Aker & Mbiti (2010) explain that whereas only a quarter of the population has electricity, 60% of the population has mobile coverage. These figures are slightly higher in South Africa where 85% of the population has access to

electricity and 95% has mobile phone coverage (Stats SA, 2013). With the increasing diffusion of smartphones and mobile Internet use (Goldstuck, 2012) comes an increasing vulnerability to attacks from cyber criminals worldwide. Dlamini *et al*. (2009) review the threats facing smartphone users, and argue that the human element is the real security challenge. Whereas a lot of effort has gone into helping companies secure their assets, personal security has not received as much attention, leaving the man and woman in the street vulnerable. According to Kritzinger & Von Solms (2010), 95% of Internet attacks involve targeting humans, not company IT systems directly. People need to be able to protect their data against unauthorized access, destruction, disclosure, and modification.

This is a position paper, presenting a literature review and concepts in order to propose a new way of making people less vulnerable, trying to improve uptake of security precautions and security software. We argue for considering society as a whole, and the role of influencers within a society, to develop individual resilience to security threats. We believe that we ought to borrow from the existing *Ubuntu* mindset to improve societal information security to nurture an *African Digital Security Culture.*

2. Poor Uptake of Security Mechanisms

Poor usability has been blamed for the meagre uptake of security products (Adams & Sasse, 1999). Yet there are other barriers to adoption too, such as those mentioned by Renaud *et al*. (2014), Harbach *et al*. (2013), Harbach *et al*., (2014) and Weirich & Sasse (2001). In the Sub-Saharan context there are additional location-specific obstacles (Prinsloo & Brier, 1996; Sayed & De Jager, 2014). Figure 1 depicts a non-exhaustive list of the barriers to adoption identified by researchers.

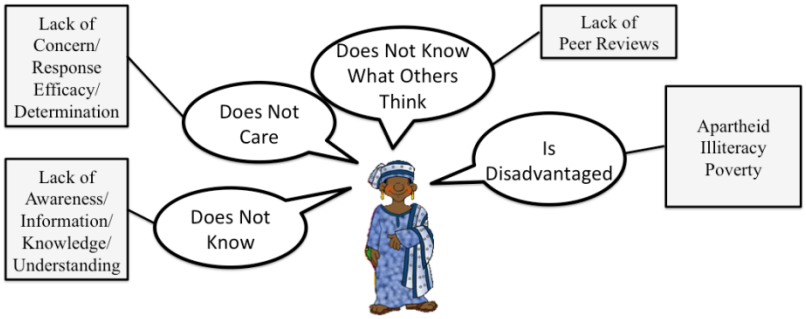

Figure 1: Barriers to Adoption of Security Precautions

To mitigate these barriers we need first to understand how to reach all South Africans, and then how to nurture a society where the idea of an *African Digital Security Culture* can be facilitated and encouraged. As mentioned before, we believe that we can nurture this culture more effectively where the Ubuntu mindset exists, since there is already a culture of adult education and community members helping each other. If we can piggy-back onto this existing mindset we might be able to help people to become more resilient.

3. Reaching Everyone; Improving Resilience

People need to know that they have an information need, be aware that there is something that they do not know, and be motivated to seek out information about a particular topic (information seeking). The former is *awareness*: something or someone making a person aware of something they knew nothing about before. Awareness has the potential to create a sense of an information need.

Having become aware of an information need, they might engage in information seeking. Case (2012) explains that information-seeking behaviour varies widely across people, situations and objects of interest so that it is difficult to predict how a particular person will go about seeking information.

It seems intuitive that people, having realised a need, will deliberately seek information from formal sources. Intuition is wrong in this case. In the first place it seems that information is gathered in passing, without the person even seeking it out (Babin *et al*., 2010). The literature suggests that much of what constitutes 'everyday knowledge' comes from our interactions with other people within our society (Bruner, 1990), not as a consequence of deliberate information seeking.

If people *do* deliberately seek out information it seems that they prefer to obtain information from friends and family (Case, 2012; Babin *et al*., 2010). There is a widespread myth that media has a significant impact on the public's thoughts, feelings and actions (Stansberry, 2012). Comstock (2013) reviews a number of studies providing strong evidence that public media has a negligible impact on the hearts and minds of the public.

The next place we might intuitively think people satisfy their need for information would be by using a search engine such as Google. Much research has focused on how search engines are used, but two studies have contrasted the use of search engines and other information channels. Gray *et al*. (2005) studied health-seeking information behaviour during adolescence. They discovered that participants considered the Internet their primary source, but they also acknowledge that it is unlikely to supplant trusted peers and adults. Morris *et al*. (2010) compared the use of a search engine with querying social networks and found that the social network delivered results more quickly than a search engine.

So, there are at least two phases: *awareness* followed by *information gathering*, the latter of which can be deliberate or vicarious. There is also another phase: sharing what you know. Kuhlthau (1991) found evidence that new knowledge and understanding leads to people sharing their information with others. The role of society seems to be crucial: people learn from others and, in turn, teach others.

This is a brief review but even so it seems clear that humans are hardwired to share information and to benefit from such sharing. In essence, we learn most effectively from each other, not from books, the media, or by carrying out searches using search engines.

Case (2012) argues that too little research has focused on sharing of information between peers, and the fact that humans often avoid and ignore relevant information. Yet a literature review of peer-related security support does indeed show that many eminent researchers have started looking at this aspect of security. Rader *et al.* (2012) carried out a study to investigate how non-experts learn about security, and argue for the crucial role of the stories people tell each other in educating people about security. Ashenden & Lawrence (2013) also argue for a social marketing approach to achieve behavioural change, and Lipford & Zurko (2012) argue strongly for a social approach to security. Finally, Camp (2011) argues that usage of security software might have a tipping point, where a herd effect leads to adoption by a group of people.

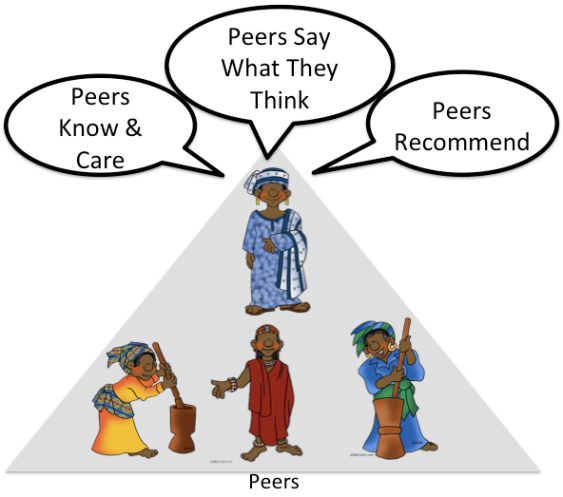

Figure 2: Societal Support

4. Nurturing an African Digital Security Culture

The key idea is that we should focus our efforts on building a security culture rather than focusing all efforts on reaching individuals. Very little effort has gone into helping the laymen and women with their digital security issues, either individually or by establishing an *Ubuntu*-like security assistance culture.

To address this obvious deficiency, an African Digital Security Culture (ADSC) for general society is proposed in order to ameliorate the risk impacts of security attacks that cannot be avoided purely by technical solutions, even if they are usable. This is because usability, on its own, does not guarantee adoption. By "society" we mean "*The aggregate of people living together in a more or less ordered community"* (Oxford English Dictionary).

Establishing a healthy ADSC might well have the potential to address the various justifications that impair the uptake of usable security mechanisms by members of society.

There is, unfortunately, no simple way to reach everyone with awareness drives, especially those in rural areas who perhaps are not proficient in English. However, there are some things that can be done. We need to ensure that the community members support each other so that people are not grappling with security issues on their own. On the contrary, knowledgeable and experienced people could support others, gradually improving the societal digital security competence. This approach has been used successfully to support weight loss (Weight Watchers) and alcoholism (Alcoholics Anonymous).

This paper's contribution is to propose an approach, leaving the validation thereof to be pursued as future work. It is proposed that we focus our attempts on developing an ADSC in three phases, the first phase being calculated to initiate an interest in members of the society (start a revolution, excite an information need). Once people realise that there is something they do not know enough about, the second phase ensures that the information need thus created can be satisfied. We need to make it easy for a community's members to find the information they seek (to satisfy the information need we have created). During the second phase we ensure that peers can recommend a secure course of action. A third phase serves to monitor the efficacy of the approach and to feed back into a new iteration of phases one and two. We will now explain the proposed approach depicted in Figure 3.

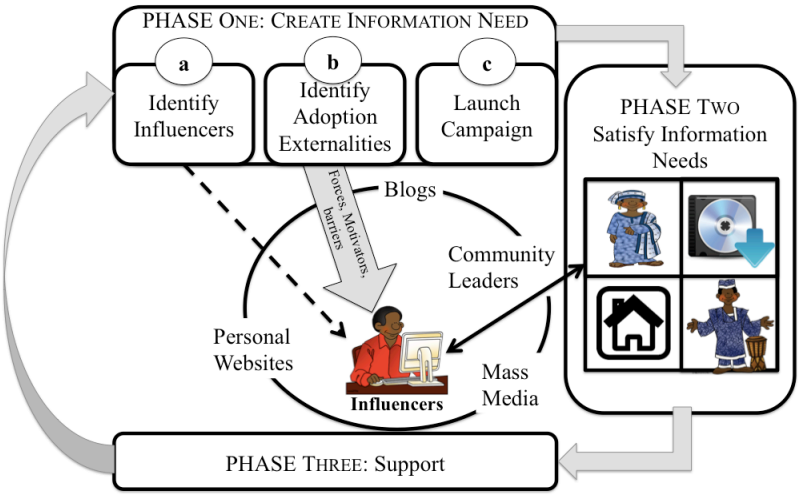

Figure 3: A Proposal for Building ADSC

4.1. Creating an Information Need (Phase One of the ADSC)

Our brief literature review made it clear that we ought not to be targeting individuals as a first step because they will not necessarily be convinced by outsiders coming in and offering advice.

The literature confirms that people learn most effectively from others in their own community. The usual approach is to provide information in the public media, make

various Web resources available, or ensure that libraries stock informative pamphlets. While these sources of information may well come into play once an information need is experienced, it is necessary first for the information need to be registered, for curiosity to be piqued, within laypeople in a society. People in a given society inhabit different networks within which they choose to spend their time. It is here that we find key people who exert an influence over the other members of the societal network. These people are called *influencers* (Kiss & Bichler, 2008). The top criteria for an influencer's role in a community is their participation level, the frequency of activity and their prominence in the community (Gillin, 2008; Zhang, 2013). Donner *et al*. (2011) already experimented with the idea of training influencers in the community to use mobile Internet in South Africa.

After this, government-sponsored intermediaries should be made available to support the network because the way people are learning (isolated from expert knowledge) means that their knowledge is often fragmented and piecemeal. This, then, is what phase two addresses, by ensuring that experts and other information sources can play a role once influencers have initiated the process (Stansberry, 2012).

Phase one includes the following steps:

(a) **Identify the influencers in a particular community**: Know the network, identify the influencers. Content of interaction is vital. The level of detail for the information is critical, so that influencers may give the right information to the people they influence.

(b) **Understand the forces, motivators and barriers to adoption**: This will help to formulate adoption strategies or how future usage can align with current values and needs (Donner *et al*., 2011; Chakravorti, 2004).

(c) **Launch Campaign**: We want to convince influencers of the benefits of the software solutions. This might need to happen face- to- face or via seminars. The aim is to ensure that they are as well informed as possible.

This exploits the theory of adoption externalities (Dybvig & Spatt, 1983). The idea is that you have to get enough influencers to start using a product so that it can diffuse through the community (Camp, 2011). This is particularly important for security products. Moreover, the training of influencers should be motivational and person-centred approach; something we learn from the drive to help people to stop smoking (Yuan *et al*., 2012).

4.2. Meeting the Information Need (Phase Two of the ADSC)

We need to satisfy the information needs excited in Phase one. Here we follow the advice of Donovan (2011) who considers the use of social marketing in promoting public health, a remotely related area to digital security. He proposes 4 P's: *price, place, promotion* and *product*, as follows:

People: Reaching people who currently do not have the knowledge and expertise to protect themselves. We do this initially via influencers.

Product: People are often flummoxed by the sheer range of products on offer. In a drive such as this one there should be a strong recommendation for one particular product. Moreover, such a product should offer simplicity and control to the adopters.

Place: Where should people go to seek information? Face- to- face word-of-mouth is the most effective route, so arranging community activities where this can take place would be a very effective launching pad to ensure that the campaign gets off to a strong start.

Politics: Target individuals who, even though they are not influencers, have the power to help people with the information need to satisfy their needs. Here people working in the community, such as librarians and teachers, can play a vital role in reaching people with vital information.

4.3. Support (Phase Three of the ADSC)

One cannot launch a campaign and then hope that it will continue without support. This is an essential component that will determine the success or failure of this security-related societal drive.

Phase three, the support phase, is grounded in the African philosophy of *Ubuntu*. Ubuntu, as explained by Eze (2005); Lutz (2009); Mabovula (2011) and Shutte (2009), embodies the "principle of caring for each other's well-being and as a spirit of mutual support". There is a collective community responsibility and Ubuntu is defined by some as "*Your pain is my pain; My wealth is your wealth; Your salvation is my salvation*". Simply put: "*I am because we are*". This phrase communicates a basic respect, compassion and support for others. The phrase "*an injury to one is an injury to all*" reinforces this community sentiment.

For developing and nurturing an African Digital Security Culture, the strengths of society and cultural philosophy, as a whole, need to be involved, supporting this initiative.

5. Conclusions

The use of pervasive computing systems, social networks, and public information systems exposes individuals to security risks. This paper discusses a number of reasons for the low uptake of usable security solutions collected from the literature.

The approach taken is that we deliberately act to complement usable technical solutions with ADSC: *common understanding and attitude, collective knowledge, common practices,* and *intuitive common behaviour* within societies. It also suggests an approach for developing and nurturing an African Digital Security Culture

(ADSC) incorporating the Ubuntu philosophy. This work is a first step in motivating a need for focusing on an ADSC. Future work will include refining the approach for developing ADSC and the development of a coherent plan for deploying the approach.

6. Acknowledgements

This work was supported, in part, by the BMBF within EC SPRIDE, the Hessian LOEWE excellence initiative within CASED, a Fraunhofer Attract grant.

7. References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.

Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa. Center for Global Development Working Paper, (211).

Babin, R., Grant, K., & Sawal, L. (2010). Identifying influencers in high school student ICT career choice. Information Systems Education Journal, 8(26), 1-18.

Bruner, J. (1990). Culture and human development: A new look. Human development, 33(6), 344-355.

Camp, L. J. (2011). Reconceptualizing the role of security user. Daedalus, 140(4), 93-107.

Case, D. O. (2012). Looking for information: A survey of research on information seeking, needs and behavior. Emerald Group Publishing.

Chakravorti, B. (2004). The role of adoption networks in the success of innovations: a strategic perspective. Technology in Society, 26(2), 469-482.

Comstock, G. (Ed.). (2013). Public communication and behavior (Vol. 2). Academic Press.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3), 189-198.

Donner, J., Gitau, S., & Marsden, G. (2011). Exploring mobile-only Internet use: Results of a training study in urban South Africa. International Journal of Communication, 5, 24.

Donovan, R. J. (2011). The role for marketing in public health change programs. Australian Review of Public Affairs, 10(1), 23-40.

Dybvig, P. H. & Spatt, C. S. (1983). Adoption externalities as public goods. Journal of Public Economics, 20(2), 231–247.

Eze, M. O. (2005). Ubuntu: a communitarian response to liberal individualism? PhD dissertation, University of Pretoria, South Africa.

Gillin, P. (2008). New media, new influencers and implications for the public relations profession. Journal of New Communications Research, 2(2), 1-10.

Goldstuck, A. (2012). Internet matters: The quiet engine of the South African economy. World Wide Worx. Pinegowrie, South Africa. Available at: http://internetmatters. co. za/report/ZA_Internet_Matters. pdf (accessed 30 September 2012.

Gray, N. J., Klein, J. D., Noyce, P. R., Sesselberg, T. S., & Cantrill, J. A. (2005). Health information-seeking behaviour in adolescence: the place of the internet. Social science & medicine, 60(7), 1467-1478.

Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013, January). On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In Privacy Enhancing Technologies (pp. 245-264). Springer Berlin Heidelberg.

Harbach, M., & Fahl, S. (2014). Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *Computer Security Foundations Symposium (CSF), 2014 IEEE 27th* (pp. 97-110). IEEE.

Kiss, C., & Bichler, M. (2008). Identification of influencers—measuring influence in customer networks. Decision Support Systems, 46(1), 233-253.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security, 29(8), 840-847.

Kuhlthau, C. C. (1991). Inside the search process: Information seeking from the user's perspective. JASIS, 42(5), 361-371.

Lipford, H. R., & Zurko, M. E. (2012, September). Someone to watch over me. In Proceedings of the 2012 workshop on New security paradigms (pp. 67-76). ACM.

Lutz, D. W. (2009). African Ubuntu philosophy and global management. Journal of Business Ethics, 84, 313-328.

Mabovula, N. N. (2011). The erosion of African communal values: a reappraisal of the African Ubutu philosophy. Journal of Humanities and Social Sciences, 3(1),

Morris, M. R., Teevan, J., & Panovich, K. (2010). A Comparison of Information Seeking Using Search Engines and Social Networks. ICWSM, 10, 23-26.

Nafukho, F. M. (2006). Ubuntu worldview: A traditional African view of adult learning in the workplace. *Advances in Developing Human Resources*, *8*(3), 408-415.

Prinsloo, M., & Breier, M. (Eds.). (1996). The social uses of literacy: Theory and practice in contemporary South Africa (Vol. 4). John Benjamins Publishing.

Rader, E., Wash, R., & Brooks, B. (2012). Stories as informal lessons about security. In Proceedings of the Eighth Symposium on Usable Privacy and Security (p. 6). ACM.

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? In Privacy Enhancing Technologies (pp. 244-262). Springer International Publishing.

Sayed, Y., & De Jager, K. (2014). Towards an investigation of information literacy in South African students. South African Journal of Libraries and Information Science, 65(1).

Shutte, A. (2009). Ubuntu as the African ethical vision. In M. F. Murove (ed.). African Ethics: An anthology of comparative and applied ethics. University of Kwazulu-Natal, press 85-99.

Stats SA (2013). General Household Survey – P0318. Pretoria: Statistics South Africa.

Stansberry, K. (2012). One-step, two-step, or multi-step flow: the role of influencers in information processing and dissemination in online, interest-based publics. Ph.D. dissertation, Journalism and Communication, University of Oregon, 2012.

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137-143). ACM.

Yuan, N. P., Castaňeda, H, Nichter, M., Nichter, M, Wind, S, Carruth, L & Muramoto, M (2012). Lay health influencers how they tailor brief tobacco cessation interventions. Health Education & Behavior, 39(5), 544–554.

Zhang, Y., Li, X & Wang, T.-W. (2013). Identifying influencers in online social networks: The role of tie strength. International Journal of Intelligent Information Technologies (IJIIT), 9(1), 1–20.