Design of a Cyber Security Awareness Campaign for Internet Café Users in Rural Areas

WA Labuschagne[1], MM Eloff [1], N Veerasamy[2], L Leenen[2] and M Mujinga[1]

[1] School of Computing, Unisa

[2] Council for Scientific and Industrial Research

wlabuschagne@csir.co.za

eloffmm@unisa.co.za

nveerasamy@csir.co.za

lleenen@csir.co.za

mujinm@unisa.co.za

Abstract: Africa may have the lowest number of Internet users in the world, but it also has the highest growth rate and the number of users is steadily growing. A majority of the African population is still excluded from global cyber networks and thus have very low cyber literacy rates. A consequence of these two factors is that many Internet users access the Internet without understanding or even realising the dangers of the cyber world. Proactive measures need to be developed to ensure that these new Internet users are equipped with computer and information security knowledge to mitigate possible cyber attacks.

Due to limited availability of infrastructure, a large percentage of the African population access the Internet via Internet Cafés. A need has been identified to make users aware of the threats that may be present at an Internet Café. This paper addresses how the National Institute of Standards and Technology (NIST) framework, defined in the guide, "Building an Information Technology Security Awareness and Training Program", can be used to develop a security awareness program that focuses on possible cyber threats at Internet Cafés. This guide provides a framework that can be applied to construct a security awareness program. It consists of four steps that form part of the life cycle of an information technology (IT) security awareness and training program. These steps are used to identify requirements of a security training strategy, to develop material that addresses the identified requirements, for the effective roll-out of the program, and to ensure the program is current and to monitor the effectiveness of the program. This framework can be used to address an identified threat in a specific context. This paper addresses the development of a security awareness campaign with the focus on reducing threats emanating from Internet Cafés.

Keywords: Internet Cafés, security awareness, security training, cyber literacy

1. Introduction

Africa lags behind the rest of the world in terms of basic telecommunication and computing infrastructure, which results in poor connectivity rates compared to non-African countries. The digital divide refers to the gap between those with regular effective access to digital technologies,

particularly the Internet, and those without [7]. Globally, the digital divide describes the gap between economically developed and developing countries, but on a national level, the digital divide often results in an urban-rural divide. In poor countries, and particularly in rural areas, most people can only gain access to the Internet through public access points such as Internet Cafés. Internet Cafés usually provide relatively inexpensive Internet access to people who cannot afford personal computers and often are unemployed.

Mutula [19] affirmed that the poor telecommunications infrastructure in Africa can be attributed to a number of factors, including governmental policies. Most African governments reluctantly freed up their telecommunications services although some still regulate these services. Regulation often hinders private companies to obtain licences to provide telecommunications services. Other factors include language barriers, lack of awareness, costs, and poor connection speeds. Mutula also mentions initiatives by the South African government to deliver affordable technology.

Otieno reported in 2010 that Africa has the lowest number of Internet users in the world. This problem prevents the majority of Africans from enjoying the benefits of digital media [21]. The current estimated statistics provided by Internetworldstats.com show the current Internet users from the African continent contribute 5.6% to the total number of Internet users in the world [12]. Furthermore, during the past decade, the number of Internet users from the African continent has grown at a rate of over 2000% [12]. These low figures could be explained due to the high cost and the limited availability of infrastructure in Africa. Twinomugisha identified the lack of infrastructure in Africa resulting in low bandwidth and high costs [25]. Africa thus has the lowest number of Internet users in the world, but it also has the highest growth rate and the number of users is steadily growing. This growth has lead to new requirements with regards to the development of infrastructure: the roll-out of the SEACOM, EASSY and TEAMS cables has significantly increased bandwidth in the African continent [25]. The SEACOM and TEAMS cables were launched in 2009 and the EASSY cable in 2010 [3, 23, 24]. Usage at Internet Cafés is likely to also increase due to the increasing availability of infrastructure. However, a large majority of the African population is still excluded from global cyber networks and has very low cyber literacy rates. Milicevic reported that more than 80% of the population of the planet is literally excluded from global information networks that provide economic, cultural, political and social interaction [17].

These factors contribute to a situation where a large number of Internet users access the Internet without knowing or even understanding the dangers of the cyber world. Proactive measures need to be developed to ensure that these Internet users are equipped with computer and information security knowledge to mitigate possible cyber attacks. In less affluent areas, the cost of Internet access and the lack of monetary means to purchase a personal computer have resulted in limited home based Internet access. A growing challenge is the creation of cyber security awareness in rural areas for Internet Café users and establishing a way through which awareness can be increased.

A security concern, for which awareness needs to be created, is the spread of malware. The nature of malware is to lure users, through the web browser used at Internet Cafés, into performing an action which will then infect the system [22]. Polychronakis et al. also noted that 68% of the users make use of portable storage devices [22]. These devices are a main attributable factor in the spread of malware. The study also revealed there is a high demand for formal training courses to educate rural users on good security practices and the dangers of malware. Security measures implemented

by employers are another important factor, identified by Kritzinger and von Solms [14]. Most corporate employees are protected by mechanisms deployed by their company to protect the users against cyber threats. In most instances these users attend computer and information security awareness programs to help them understand possible cyber attacks that they may be exposed to. A large number of companies have budgets to ensure that the best possible measures are deployed to protect their assets. On the other hand, Internet Café owners generally do not provide the same level of protection or training.

This paper addresses how the National Institute of Standards and Technology (NIST) framework, defined in the guide: "Building an Information Technology Security Awareness and Training Program", can be used to develop a security awareness program that focuses on cyber threats identified at Internet Cafés. National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce. NIST developed this Special Publication 800-50, which provides guidance for building an effective information technology (IT) security program [26]. This guide provides a framework that could be used to conduct a successful security awareness program; it addresses four critical phases that form part of the life cycle of an IT security awareness and training program. These phases are used to identify a need for a security training strategy, the development of material that addresses the identified needs, the effective roll-out of the program and steps to ensure the program is current and monitors the effectiveness of the program.

The remainder of this paper is structured as follows: Section 2 gives some background on Internet Cafés in rural areas, Section 3 discusses the NIST framework, Section 4 considers issues surrounding security awareness levels of Internet Café users, and in Section 5 the NIST guidelines are applied to develop a framework for a security awareness campaign for Internet Café users in rural areas. Section 6 concludes the paper.

2. The Internet Café Industry in Africa

An Internet Café is a privately owned business that provides access to the Internet, as well as the usual services of a traditional café such as coffee and snacks. The first Internet Café was opened in London in 1994 [2]. In the United States, a business that provided coin-operated computers with dial-up access to the Internet was launched as early as 1991. The first actual Internet Café in the US opened in 1995 in Chicago.

Hyde-Clark [11] claims that the first South African Internet Café, The Milky Way Café, was opened in Johannesburg in December 1994. Limited statistics regarding growth rates and current numbers of Internet Cafés in Africa exist, but we give a short summary of a few relevant studies. Mutula [19] reported in 2003 that there was significant growth in the industry in South Africa from 1999. Molowa [18] also notes that the industry is growing at a high rate in South Africa, but he does not provide statistics. Mwesige [20] notes that Uganda has seen a rapid growth of Internet Cafés, although at the time of this report, the growth was mostly in the capital city, Kampala. The first Internet Café started in 1996 in Uganda.

There are a number of studies on the nature of Internet Cafés and their users in rural and urban areas, as well as in affluent and poorer areas. A few examples from these studies are provided in the following paragraphs.

Two studies that focus on Internet Cafés in Johannesburg cite differences in the Internet usage and costs in affluent and poorer areas. Hyde-Clarke [11] compares two Internet cafés and notes that the rates charged by the Internet café in the more affluent area are significantly higher than the café in the poorer area. He also notes that users in the more affluent area mainly use the Internet to expand existing business activities, while users in the poorer areas tend to use the Internet to search for employment or to attempt to establish business contacts. In addition, Hobbs and Bristow [10] studied a number of Internet Cafés in both affluent and less affluent areas in Johannesburg. They found that there are more Internet Cafés in less affluent areas. This is likely because poorer people are less likely to have their own personal computers. Another observation is that 64% of users in the study used more than one Internet Café, and that 65% of users have a high rate of repeat usage. Another important observation is that there is a high demand for training at cafés and that fellow users often offer assistance or informal training to less competent users, or that some users access the Internet on behalf of other people who do not have the required skills.

From a wider perspective, Furuholt and Kristiansen [7, 8] studied Internet Cafés in Indonesia and Tanzania and compared the industry in these two developing countries. They also note that in developing countries, most Internet users gain access to the Internet through public access points such as Internet Cafés. In their study on cafés in Tanzania they found that there are 16 times more people per Internet Café in rural areas than in urban Dar es Salaam. They also find that rural users on average have one third of the income of their urban counterparts, but they spend almost the same amount of money at Internet Cafés. In their comparative study of Tanzania and Indonesia, they found that although these two countries are at different levels of development, their Internet Café users are remarkably uniform. In both these countries, Internet Café users tend to be poor but spend a high percentage of their income on Internet Café services. The main activity is to read and write emails, but the cafés serve a role as training facilities. Internet Café staff can therefore be used to provide training and awareness to less educated people.

Furthermore, Mwesige [20] reported in his study of Internet Cafés in Uganda that very few residents owned a personal computer and access to the Internet is mostly provided by public access points such as Internet Cafés. He also reported that repeat usage is very high in Uganda and that users in cafés mostly accessed their email.

Overall, Furholt and Kristiansen [8] give an overview of studies on the industry globally, but the results that are relevant in our context support the observations we mention above. These observations are relevant to an awareness campaign because:

- The Internet Café is often the only access point for a rural, poorer person. Such a user is possibly unemployed and may not have had exposure to security awareness campaigns.
- There exists a need for training at Internet Cafés and this requirement implies that there probably exists a lack of cyber security awareness. A high percentage of Internet Café users are repeat users. Repeat users can contribute to reliable participation in an awareness campaign. If we apply this trend to the generally less affluent rural environment, we can conclude that decentralised Internet access exists and this could affect the reach and impact of an awareness campaign.

It has been identified that the NIST framework would serve as an ideal guide to implement an awareness campaign for Internet users in rural areas. In the next section, a high-level overview of the NIST framework is provided.

3. The NIST guide to develop a Technology Security Awareness and Training Program

The National Institute of Standards and Technology has developed a framework that aims to guide the development of an Information Technology (IT) security program. In this study, the framework is used to design a campaign to create cyber security awareness in Internet Cafés in rural areas. This section contains a summary of the NIST framework so as to provide the context for the work in the other sections [26].

The NIST framework consists of four high level steps. Figure 1 shows a summary of the relevant steps of the NIST framework to guide the development of a cyber security awareness campaign. A short summary of each step follows.

3.1 Designing an Awareness Program

To design an awareness program, a needs assessment needs to be carried out. The following issues pertain to a needs assessment:

- A needs assessment is a process that can be used to determine an organisation's awareness needs.
- It is important to consider the motivation and methodology to conduct a needs assessment.

The outcome of a needs assessment is an understanding of security issues that will help shape the strategy and design of the IT security awareness program.

3.2 Developing Awareness Material

The issues to consider when developing awareness material are the selection of the awareness topics, as well as the sources of developing the awareness material. The development of the awareness material is dependent on the needs assessment. The needs assessment will identify the topics which need to be addressed when developing the awareness material.

3.3 Implementing the Awareness program

To implement the awareness program, a selection will be made of the techniques through which the messages will be delivered. The chosen techniques will depend upon resources and the complexity of the messages. Techniques for effectively delivering training material should take advantage of technology that supports:

- Ease of use;
- Scalability;
- Accountability;

- Broad base of industry support.

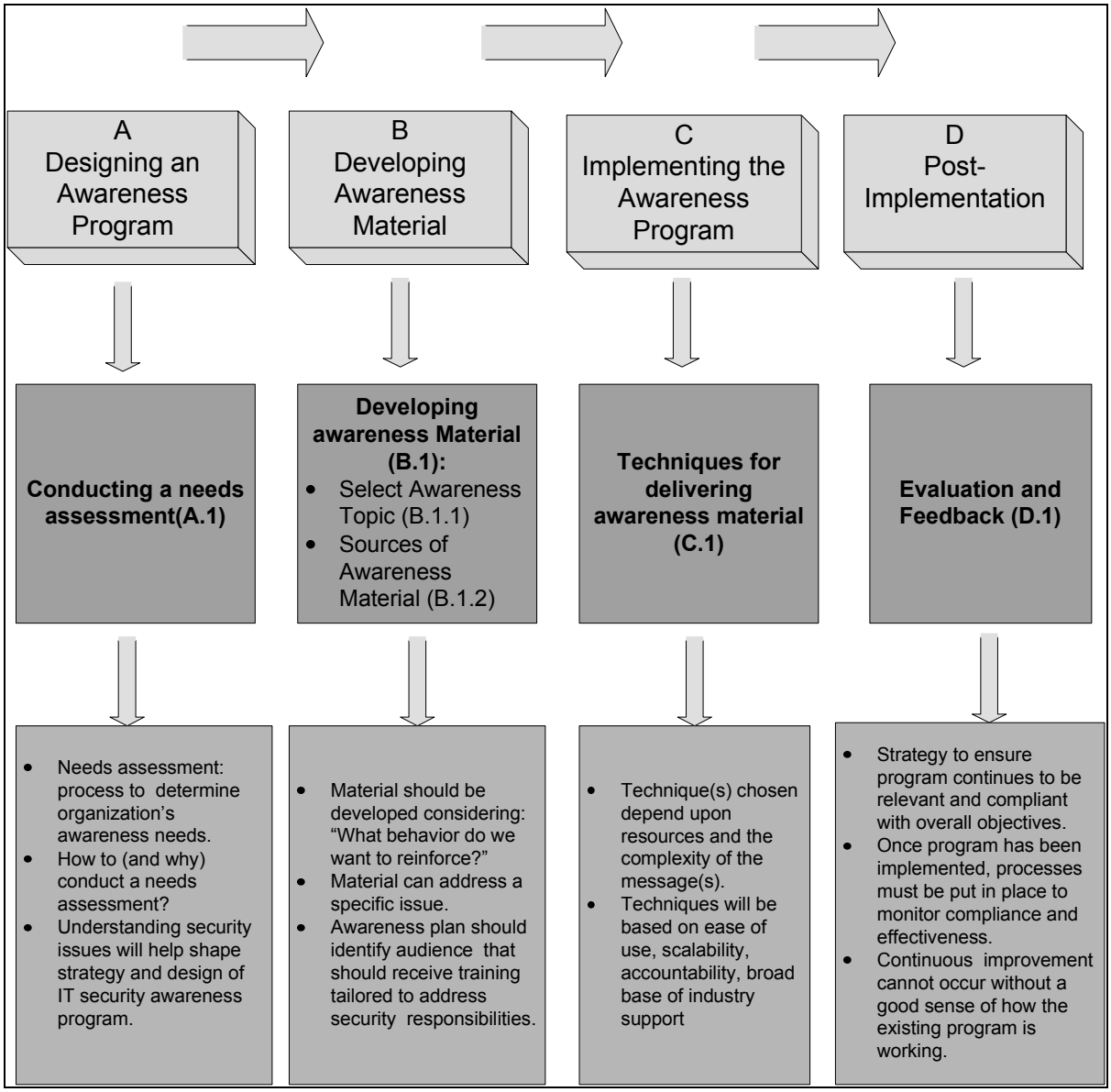

Figure 1: High-level outline of NIST framework

The different means of transferring security knowledge are through the use of formal training sessions, strategic placement of awareness messages, passive computer-based, web-based, and interactive computer based training. Problems have been identified to hold a user's attention due to the passivity of the knowledge transfer. Formal training sessions can be conducted by an instructor who will use material like books and presentations to transfer the content to the users. This method does not involve the participation of the user and is usually seen as one-way communication. The knowledge attained during these types of sessions may be quickly forgotten once the sessions are completed. Computer based training is where the user is exposed to the information via a computer and learning is conducted in their own time. Knowledge is only transferred to the user and the application of the knowledge is never used in real applicable situations. This does not imply that the knowledge gained will be retained over a long period or will be applied in a situation whereby the knowledge would be useful to resolve a problem.

The use of awareness messages is helpful to make people aware of certain knowledge. This can be done with the use posters, screen savers or emails that contain security related information. However, similar to computer based training methods, the publication of awareness messages does not imply that the knowledge is retained or guarantees that the information was understood.

A good method to transfer and provide a platform where the information can be useful, is with the use of interactive computer based training. It provides information and ensures that learning does take place, due to the active interaction. This medium can ensure that knowledge gained is used in the right context in the right environment. The trainee can obtain immediate feedback based on the actions required to solve a problem. Video games are interactive computer based training, and examples include CyberCIEGE and CyberProtect. Both these tools can be used to transfer cyberspace security knowledge.

Thus, during the implementation of the awareness program, a decision will need to be taken with regards to the delivery method. Issues regarding interaction requirements and retention strategies will be taken into consideration.

3.4 Post-Implementation

During the post-implementation phase, the security awareness program can be evaluated. Once the program has been implemented, processes must be put in place to monitor compliance and effectiveness. The feedback loop provides a strategy to ensure that the program continues to be relevant and compliant with the overall objectives. Continuous improvement cannot occur without a good evaluation of how the existing program is working. Assessments after an awareness campaign can be used to determine if any knowledge has been effectively acquired during the learning process.

3.5 Summary

This section provided a short summary of the NIST framework. It highlights the main phases to be implemented when designing a security awareness program. The next section addresses the application of the NIST framework to the design of a cyber security awareness campaign for Internet Café users in rural areas.

4. Design of a Cyber Security Awareness Campaign

In this section, we apply the NIST framework to design a security awareness program for Internet Cafés in rural areas. Each of the steps described in Section 3 will be applied sequentially, in order to explain how a cyber awareness campaign for Internet users in rural areas can be developed. The initial step is the completion of a needs assessment to initiate the design of the awareness campaign. The description of the needs analysis follows in the next section.

4.1 Conducting a Needs Assessment

With reference to Figure 1, the initial step in the NIST framework is the Design of the Awareness Program. This is achieved through a needs assessment. The needs assessment process can be carried out by:

- Interviewing Internet Café owners.
- Literature study of attack vectors at an Internet Café.
- Observation and identification of threats.

Threats are considered as the source/person/organisation that seeks to breach security and benefit from an exploitation attempt. An attack vector is the medium through which the threat is exploited and can thus be considered as a vulnerability or weakness of the system. Attack vectors are relevant as they be will used in the development of awareness material when the means through which a threat can be exploited, will be explained to the user. Therefore, it is essential to consider both the threats and the attack vector. Core to the needs assessment and the completion of attack vectors is a literature study to identify threats and Internet uses.

4.1.1 Identification of Internet Uses

Furuholt and Kristiansen discuss the various uses of the Internet [7, 9]. In order to complete the mapping of the attack vectors covering threats and Internet uses, the findings of Furuholt and Kristiansen are further classified as a means of abstraction for future application. Social Networks are included as an additional Internet use. Table 1 was generated by listing Internet uses and then classifying a use into a high-level categorisation. This provides a level of abstraction for the compilation of the mapping of attack vectors.

Table 1: Internet Use Classification

Type of Use	Classification
Seeking information	Information
Email	Communications
Chatting	Entertainment
Reading online news	Information
Research	Information
Computer games	Entertainment
Downloading software for professional use	Business
Downloading software for amusement	Entertainment
Downloading music	Entertainment
Visiting pornographic sites	Entertainment
Doing business	Business
E-shopping	Financial
Gambling	Financial
Social networks	Communications

4.1.2 Identification of Threats

The use of the Internet is far-ranging and spans functionality from communication to entertainment. Such functionality also brings with it associated threats that can be exploited and should therefore be considered in a needs assessment. A literature study on Internet threats in rural areas is therefore carried out next.

Firstly, the works of Anselmi, Menon, Won, Evans and Manning are considered collectively. Identified threats include: worms, Trojans, password/info stealers, adware, backdoors, viruses, exploits, spyware, phishing, downloaders, droppers, ransomeware, social engineering and rootkits [1, 4, 13, 15, 16].

Furthermore, the works of Akhil and Evans also discuss threats like browser based attacks and social media/social web [5, 16]. Browser based attacks can be elaborated into specific vulnerabilities on the following platforms: Firefox, Internet Explorer, PDF, SWF, ActiveX and MS Office.

Moreover, when considering the works of Evans, Kim and research from F-Secure, the following threats emerge: identity theft, spam, hacking, denial-of-service, violation of digital property rights and cyber bullying [4, 6, 13].

Various threats that are critical to Internet Cafés in rural areas were thus identified. These threats should be adequately reflected in the needs assessment to design a cyber security awareness campaign for Internet Cafés in rural areas. In the next section a mapping is given of threats and uses as part of the needs assessment process.

4.1.3 Mapping of Internet uses and threats

In Table 2, a sample mapping is shown of Internet uses to prominent threats. This serves to show the relation between critical threats and their functionality in core Internet uses. The identification of the crucial threats to Internet users in rural areas will be used to determine appropriate topics for the development of awareness material, which is the next step in the application of the NIST framework.

In Table 2 the Internet uses are ticked as columns of the corresponding threats as a means of showing their application. Certain threats were clustered together under a high-level banner to demonstrate that their core underlying functionality could be grouped. For example, malware is the high-level classification for viruses, adware, scareware, spyware, worms, Trojans, password/info stealers, backdoors, downloaders, droppers and rootkits. Browser- based threats were broken down into Firefox, Internet Explorer, PDF, SWF and MS Office. Hacking (exploits) was considered as the high-level category that social engineering, inherent software vulnerabilities and patch management could correspond to.

The legends indicated in Table 2 denote the applicability of the threats to the uses at Internet Cafés. The symbol ‘X’ denotes “not applicable”. An example is that physical harm cannot occur from using an Internet Café to search for information on the Internet. The tick symbol denotes that the threat is applicable to the given use. An example of this scenario is a Web Browser that can be exploited via a vulnerability when using it for entertainment purposes. The symbol ‘P’ denotes “partial applicability”. This is used to indicate that the threat can apply only in certain circumstances. An

example is a phishing attack where a user's information can be harvested by searching for information. Some web sites require the user to provide personal details to obtain access to the content. The user can not verify that the web site would adhere to a policy to not share the captured data with external entities.

The various types of malware and browser-based threats, for example, span all the uses of the Internet and therefore a tick is indicated for each of the threats. Similarly, spam is another threat that covers all the Internet uses because a user chatting, using email or when signing up to download music or software has the potential to be spammed. The same principle applies when access to information resources is prevented due to a denial of service (DOS) attack.

Software has inherent flaws that can be exploited in order to take advantage of systems. Software is used in almost every application from email to downloading music and gaming. Thus, it is evident that the threat of inherent software vulnerabilities is applicable across all uses of the Internet. This also implies that patch management would mitigate possible exploitation of the software, preventing interruptions of operations at the Internet Café. Patch management is therefore also applicable to all uses of the Internet as updates are relevant to the various uses of the Internet.

Furthermore, threats that have a psychological perspective are also relevant to users in Internet Cafés in rural areas. Users can divulge information that could assist attackers to physically locate them, entice them to provide more personal information or convince them to perform actions that they would not have done under normal circumstances. Data could be collected during an online chatting session or with the use of social networking sites that record geo-location data posted by the user. This can eventually lead to physical harm if the user is tracked down and attacked based on information collected online. The Internet provides platforms where users can be hurt or be embarrassed: text or images could be sent or posted to intentionally spread false and negative information. The viral nature of the Internet will spread the information beyond the control of the person who posted the information. The use of the Internet for communication and entertainment is important components for people to stay in touch. However, care should be taken in what data people share on these platforms. Threats like cyber bullying, physical harm and the spreading of negative information are mainly relevant to the use categories of entertainment and communications as the mechanisms of chatting computer games, signing up for music or software for one's own amusement, social networks and email fall into these categories.

Moreover, techniques like social engineering also rely on influence to lure or trick users into performing an action by creating a relationship and then taking advantage of the trust created to manipulate the user. The user can be lured into unintentionally providing more personal information by visiting a phishing site or becoming the victim of a scam. The attackers could use the trust already established to trick the user into making payments for products or services with the intention not to provide the actual services. The faceless characteristic of the Internet creates these devious opportunities. Data collected during a phishing attack can be used to impersonate a user. Identity theft provides attackers with avenues to conduct financial transactions without establishing the validity of the credentials of the person. Phishing, identity theft, online scams and fraud are devised by the user's participating in a two way communication and providing data that can be stored and later used by attackers. Phishing and online scams are mainly relevant to financial, business and

communication uses of the Internet. Identity theft has partial applicability to business and entertainment uses, but is still applicable to financial and communication uses.

Table 2: Mapping of Internet Uses to Threats

Use/Threat	Info	Entertainment	Financial	Business	Communications
Spam	✓	✓	✓	✓	✓
DOS	✓	✓	✓	✓	✓
Phishing	P	P	✓	✓	✓
Violation of digital property rights	✓	✓	X	✓	P
Malware					
Virus	✓	✓	✓	✓	✓
Adware	✓	✓	✓	✓	✓
Scareware	✓	✓	✓	✓	✓
Spyware	✓	✓	✓	✓	✓
Worms	✓	✓	✓	✓	✓
Trojans	✓	✓	✓	✓	✓
Password/Info stealer	✓	✓	✓	✓	✓
Backdoor	✓	✓	✓	✓	✓
Downloader	✓	✓	✓	✓	✓
Dropper	✓	✓	✓	✓	✓
Rootkit	✓	✓	✓	✓	✓
Browser Based					
Firefox	✓	✓	✓	✓	✓
IE	✓	✓	✓	✓	✓
PDF	✓	✓	✓	✓	✓
SWF	✓	✓	✓	✓	✓
ActiveX	✓	✓	✓	✓	✓
Opera	✓	✓	✓	✓	✓
MS Office	✓	✓	✓	✓	✓
Hacking(Exploit)					
Social engineering	X	✓	✓	✓	✓
Inherent software vulnerabilities	✓	✓	✓	✓	✓
Patch management	✓	✓	✓	✓	✓

Use/Threat	Info	Entertainment	Financial	Business	Communications
Online scams and fraud	✓	P	✓	✓	✓
Physical harm	X	✓	X	X	✓
Cyber bullying	X	✓	X	X	✓
Spreading false or negative information	X	✓	X	X	✓
Illegal online gambling	X	X	✓	✓	P
Identity Theft	X	P	✓	P	✓

In addition, the Internet also poses various threats that may have legal implications. Internet Café users can download copyrighted software, music, books or content that infringes on digital property rights and these offences may be punishable. Legal and regulated gambling sites may not provide sufficient winning margins which means users may search for unregulated gambling sites that provide higher winning margins. These sites are created for the black market where cyber laws may not be adhered to. Prosecution of unlawful action is not always possible, for example in the 419 scams users were tricked to deposit large amounts of money and the operators of the sites disappeared without providing a service. Online scams and illegal online gambling are mainly applicable to the business and financial uses of the Internet.

The main aim of mapping the Internet uses to threats is to identify and prioritise critical topics that are essential for the cyber awareness campaign. The mapping provides a method of ascertaining which threats are pertinent to users of Internet Cafés in rural areas. This output will feed into the next step of applying the NIST framework: Developing Awareness Material.

4.2 Develop Awareness Material

To develop the awareness material, information gathered from the needs assessment will be utilised to select awareness topics. The topics can then be researched in order to develop the content.

The content of an awareness program is determined by the needs that have been identified. The identification process described in Section 4.1.3 produced a list of potential threats that can be encountered at Internet Cafés. The different threats can be studied to determine those that will have the highest impact on the users at Internet Cafés. A discussion follows on the relevance of certain threats to users of Internet Cafés in rural areas. The discussion commences with the elimination of certain threats by explaining why they are not priority topics of awareness creation for users of Internet Cafés in rural areas. The discussion then moves on to relevant threats for which awareness should be created.

4.2.1 Motivation for elimination of threats

While spam can be encountered with all the uses identified at Internet Cafés, the mitigation of these attacks is not part of the knowledge and skill set of an average Internet Café user. These users usually will connect to their email using a web browser. Spam filtering is part of the services provided by the email providers and the user has no control over this. While the users can reactively

create rules to discard certain spam messages, it is the service provider who is required to provide protection at a higher level. The user also has no control over a denial of service attack. These attacks occur when attacker utilises services to prevent users accessing resources on the Internet. The violation of digital property rights is not a high priority threat as not all Internet Cafés provide the service of creating duplicate copies of digital content with the use of burners. Extra hardware would be required which will have a financial impact and the owners of these establishments could be liable for the violation of digital property rights.

Users make use of browsers to access the Internet at Internet Cafés. Browsers are software with inherent vulnerabilities which requires updates or patches to provide security to the users. The browsers are utilised third party software to provide additional functionality. For example a web browser can use Acrobat Reader to open a PDF file in the browser. This will allow the user to read the file. Ensuring that the browser is fully updated with the latest patches, does not ensure that the third party software is updated. Due to the technical nature, this threat should be mitigated by the technical team of the establishment.

Malware is a prevalent threat which affects all the uses at an Internet Café. The different types of malware as described in Table 2 can be executed on a system by a user. Users can be lured into performing these actions with or without their knowledge. Certain malware, for example, downloaders, droppers and Trojans, can be installed on a system by simply visiting a web site with a vulnerable web browser. The other malware can be installed by users executing malicious software. For example, viruses or worms could use the network to identify vulnerabilities on systems on the network and infect the systems. Malware infections can be mitigated by using software that provides protection on these levels. In the context of the Internet Café, the establishment should ensure that these protection tools are available and updated.

4.2.2 Motivation for applicability of certain threats

The remaining threats: phishing, social engineering, scams, cyber bullying, physical harm, spreading false or negative information, illegal online gambling and identity theft are recommended topics for security awareness programs for Internet Café environments. Users can decide on the actions they perform and no technical skills are required to mitigate these threats.

The purpose of an awareness program is to provide users with the knowledge to identify and mitigate these threats. Using casual chains it is possible to identify that social networking sites and email are uses of the Internet where these threats are predominant. The potential exploitation when using the Internet for email and social networking, are applicable topics for awareness creation to most Internet Café users as information that is disclosed can be used to attack users and perform other attacks on the infrastructure of the establishment. For example, personal information could be used to spread false information or used in a cyber bully attack or collect data to perform a social engineering attack. Localisation information could be used to determine the physical location of a user at a specific time which could create an opportunity for physical harm.

Attackers could implement influence techniques to trick users into performing actions or participating in events that affects the users negatively. Users at Internet Cafés are prime targets for emails that can be used to promote illegal online gambling, being lured into scams and phishing

sites. For example, a user can receive an email from an illegitimate financial establishment. The content of the email will look authentic. An uninformed user will implicitly trust the email and comply with the request in the email by clicking on the link and providing data requested. A user who is aware of phishing attacks would have looked at the source of the email, the legitimacy of the address of the web site and be aware that no financial establishment would request authentication information in an email. Furthermore, data collected from phishing sites can be used for identity theft.

Therefore, based on the previous discussion, the issues identified as most critical for which material should be developed for an awareness campaign for users in Internet Cafés in rural areas are: phishing, social engineering, scams, cyber bullying, physical harm, spreading false or negative information and illegal online gambling. The next step addresses the implementation of the awareness program.

4.3 Implement the Awareness Program

Awareness material can be delivered to users via Interactive video training (IVT), web-based training, non-web computer-based training, or instructor-led training.

The nature of an Internet Café influences the method used to deliver the awareness program. In Section 3.3 the different types of delivery methods were discussed. They include formal training sessions, strategic placement of awareness messages, passive computer-based, web-based and interactive computer based training. In this application of the NIST framework, the placement of awareness messages and passive computer based training will be more effective in Internet Cafés. The users will not be distracted from the initial intention of using the services at the Internet Café. Computer based training modules could be installed on the computers which will allow the users to use it when required. Formal training session and discussion groups are not suited for an Internet Café, as these types of delivery methods will impede on the users' need to use the Internet services provided.

After studying the various mediums for delivering material, a selection will be chosen depending on the resources and complexity of the message. In this case study, the use of posters, screen savers, a message of the day, or a pop-up message on the computer can be chosen to deliver content to the Internet user.

The topic chosen for awareness creation in this example, Phishing, can be explained to users as emails sent with malformed URLs imitating legitimate banking, financial or shopping services. This message can be designed to appear in a pop-up message or screen saver.

4.4 Post-Implementation

Thereafter, the awareness campaign can be evaluated to determine whether it was effective in educating users. Feedback and evaluation can be carried out through:

- Interviews to determine awareness levels.
- Questionnaires to determine awareness levels.
- Analysis of online behaviour to determine if phishing sites were visited.

5. Conclusions

This paper discusses the use of the NIST framework to design cyber security awareness programs for Internet Café users in rural areas. The authors motivate that there exists a dire need for security awareness among Internet Café users, and especially Internet Café users in rural African areas. Africa has the lowest percentage of Internet users in the world and it has poor telecommunication infrastructure. These factors combined with poverty, especially in rural areas, lead to Internet Café being the only access point for a majority of rural Africans. These Internet users are often unemployed and will thus not have access to security awareness programs delivered by larger businesses. Internet Cafés provide the means for the less fortunate to empower themselves by accessing online services and acquire knowledge from the content available on the Internet. Unfortunately accessing the Internet is a double-edged sword and with all the advantages of the Internet, also comes the dangers of the cyber world to the uninformed user.

Some frameworks exist to create security awareness programs to address the dangers that are present at these establishments. The NIST framework consists of sequential steps that identify a need through the collection of information and the subsequent development and delivery of the content which address the inadequacy of security awareness demonstrated by users and owners at Internet Cafés. The framework also provides a mechanism to evaluate the success of the security awareness program. However, this paper addresses the feasibility of the framework to identify content specific for Internet Cafés. The application of the framework in this paper identifies the different usages of Internet Cafés and the different threats that can be encountered at these establishments. Furthermore, an analysis of the identified uses and threats provide a summary of security related topics that are specific to Internet Cafés. Some of these topics include, but are not limited to, Phishing, social networking, spam, malware, identity theft and browser based attacks. The Internet is an ever-changing landscape and with the technology evolving so do the threats. Internet users should be empowered to be able to mitigate these threats. Users can access the Internet from different access points. This paper addressed a process of using a framework to create a security awareness program to address threats at one of these access points, namely the Internet Café.

References

[1] D. Anselmi and R. Boscovich, "Microsoft Security Intelligence Report," Microsoft, Tech. Rep. 9, pp. 1-76, 2010.

[2] Cyber Internet Café, "Internet Café History", Accessed 20110307, Available online at http://www.cyber-internet-cafe.com/internet-cafe-history.html.

[3] Chanel De Bruyn, "EASSy undersea cable launched, capacity almost trebled", Engineering News, Accessed 20110303, Available online at http://www.engineeringnews.co.za/article/eassy-undersea-cable-launched-capacity-almost-trebled-2010-08-05.

[4] J. Evans, "A Brief Analysis of the Cyber Security Threat," Hacking9, vol. 5, issue. 11/2010(36), pp. 46-49, 2010.

[5] J. Evans, "The Social Web Threat," Hacking9, vol. 6, issue. 01/2011(37), pp. 46-49, 2011.

[6] F-Secure, "Threat Types", F-Secure, Accessed 20110304, Available online at http://www.f-secure.com/en_EMEA-Labs/virus-encyclopedia/articles/classification/threat-types.html.

[7] B. Furuholt and S. Kristiansen, "A Rural-Urban Divide? Regional Aspects of Internet Use in Tanzania", Proceedings of the 9th International Conference on Social Implications of Computers in Developing Countries, 2007.

[8] B. Furuholt and S. Kristiansen, "Internet Cafes in Asia and Africa - Venues for Education and Learning?", Journal of Computing, vol. 3, 2007.

[9] B. Furuholt, S. Kristiansen and F. Wahid, "Gaming or gaining? Comparing the use of Internet cafés in Indonesia and Tanzania", The International Information & Library Review, vol. 40, pp. 129-139, 6 2008.

[10] J. Hobbs and T. Bristow, "Communal computing and shared spaces of usage: a study of Internet cafes in developing contexts", ASIS&T IA Summit, Las Vegas, March, pp. 22–26, 2007.

[11] N. Hyde-Clark, "The Urban Digital Divide: A Comparative Analysis of Internet cafes in Johannesburg", Review of African Political Economy, vol. 33, 2006.

[12] Internetworldstats, "Internet Usage Statistics for Africa", Accessed 20101111, Available online at http://www.internetworldstats.com/stats1.htm.

[13] W. Kim, O. Jeong, C. Kim and J. So, "The dark side of the Internet: Attacks, costs and responses", Information Systems, Elsevier2010.

[14] E. Kritzinger and S.H. von Solms, "Cyber Security for home users: A New Way of Protection through Awareness Enforcement", Computers & Security, vol. 29, pp. 840-847, November Elsevier2010.

[15] R. Manning, "Phishing Activity Trends Report," Anti Phishing Work Group, Tech. Rep. 2nd Quarter, 2010.

[16] A. Menon and M.G. Gabrielv, "State of the Internet 2010: A Report on the Ever Changing Threat Landscape," CA Technologies, 2010.

[17] M. Milicevic, "Cyberspace and globalization", Paper presented at CSIR Conference Centre, Pretoria, South Africa, Accessed 20110307, Available online at http://www.ais.up.ac.za/digi/docs/milicevic_paper.pdf.

[18] S. Molawa, "The First and third World in Africa: Knowledge Access, Challenges and Current Technological Innovations", Proceedings of the 1st International Conference on African Digital Libraries and Archives, 2009.

[19] S.M. Mutula, "Cyber Cafe Industry in Africa", Journal of Information Science, vol. 29, 2003.

[20] P.G. Mwesige, "Cyber elites: a survey of Internet Café users in Uganda", Telematics and Informatics, vol. 21, pp. 83-101, 2 2004.

[21] J. Otieno, "Africa: Low Internet Usage the Bane of Africa's Digital Media", Accessed 201011/18, Available online at http://allafrica.com/stories/201003190904.html.

[22] M. Polychronakis, P. Mavrommatis and N. Provos, "Ghost turns zombie: exploring the life cycle of web-based malware", in Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, pp. 1-8, 2008.

[23] Seacom, "Seacom goes live", SEASCOM, Accessed 20110303, Available online at http://www.seacom.mu/news/news_details.asp?iID=100.

[24] TelecomPaper, "Teams cable launches in Kenya", Telecompaper, Accessed 201103/03, Available online at http://www.telecompaper.com/news/teams-cable-launches-in-kenya.

[25] A. Twinomugisha, "Why Are African Internet Access Prices Still High?", Accessed 20100209, Available online at http://www.africabusinesssource.com/experts/why-are-african-internet-access-prices-still-high/.

[26] M. Wilson and J. Hash, "Building an information technology security awareness and training program", NIST Special Publication, vol. 800, pp. 50, 2003.