Designing user security metrics for a security awareness at Higher and Tertiary Institutions

Fungai Bhunu Shava
Lecturer Polytechnic of Namibia
Windhoek, Namibia

Darelle Van Greunen
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa

Abstract

Information security is at the heart of every organisation or individual who uses Information and Communication Technology (ICT) devices to socialize or for business. Security aims to ensure that users experience the three main goals of security: confidentiality, integrity and accountability (CIA). Despite the importance of security, very few organisations have proper plans to create awareness among their employees. Information security requires the user to be aware of the existence of security features on their electronic devices and to be able to use them appropriately. In a quest to establish the underlying reasons for increased exploitation despite the efforts in security solutions design, the focus is on awareness as a major factor influencing human behaviour. Online surveys were conducted to investigate security awareness levels in a case site. The case study was at an institution of higher and tertiary education in Namibia. Document review on security trends and approaches from selected leading industries was also done. Results show that most users are not aware of security policies operational in their organisation. In this paper we outline the security metrics that guide in formulating security awareness strategies.

Keywords
Security awareness, metrics, policy awareness
Introduction

Security awareness is the ability of a user to understand and implement security policies in programmes or organisations (Hubbard, 2002). According to Wilson and Hash (2003), awareness is meant to enable users to identify IT security concerns and to behave appropriately. Security depends mainly on user behaviour as most of the security actions depend on end user choices to act or not to act on security messages. To protect information and IT infrastructure, the organisations need to have policies in place and to educate the users about them. Successful implementation and evaluation of security depends on the success of user education. NIST 8800-12 agrees that security responsibility awareness for users as well as training them on security best practices will change user behaviour (2007).

Most organisations have security policies; however, their users are not aware of the policies or the meaning and implications of implementing them. An extract from ISO/IEC17799:2005 section 8.2.2 on Information security awareness, education and training recommends that all end users ought to receive suitable awareness training and regular updates in organizational policies and procedures, as applicable to their job function.

Primarily, computer users log onto a computer system to communicate for social or business purposes, to share information and to get information from the World Wide Web. Among the people who communicate or share information or make information available for other users to download are cyber criminals. Cyber criminals capitalize on user behaviour when they access information on the web (2005).

Access to information has evolved and nowadays includes: the cloud and mobile devices of all sorts. To access information conveniently, users tend to use removable devices (currently, USB devices), and multiple mobile devices. We argue that this provides convenience as the users are empowered to access their information always, anywhere. Furthermore, applications are designed to enhance the user interaction with technology. However, this convenience comes with a price as each device has its own inherent security weakness. Is the user aware of these weaknesses and of ways to protect themselves? The focus of this paper is to identify the main security threats which users should be aware of and to rank the risk they pose to the users. The importance of security policy, security awareness and human factors that can be used as metrics to enumerate the security in an organisation are discussed. The paper aims to answer 3 research questions. The main research question is: How can the security metrics be used to come up with a security awareness strategy for a higher and tertiary institution? The research sub questions include:

What is the security awareness level among the case site community?
Which metrics can be used to measure the security awareness baseline?

This paper presents security metrics which can be used to evaluate the baseline security awareness of individual users before implementing awareness programs. The structure of the paper presents background information on information security awareness and security threats, objectives, methodology, findings, recommendations and conclusions.
Information Security Overview

The most important components of Information security are technology, process, policy and culture. ISO/IEC 27002 defines 12 security domains, namely: security policy, asset management, organizing information security, human resources, physical and environment, communication and operations management, access control, information system acquisition, development and maintenance, information security incident management, business continuity management and compliance. The 12 security domains are important when defining security metrics and coming up with security awareness strategies. We have borrowed from the domains in drawing up the security awareness metric that is the human resources component.

The importance of awareness cannot be ignored if security is a goal. Security awareness deals with the human resources security domain of the ISO/IEC 27002 guideline or code of practice. Furnell, Jusoh, and Katsabas (2005) made recommendations for improving user security, including user training on: application security and how best to use it, security threats one is exposed to when one connects to a network and how to manage those. Current research trends still allude to the fact that the human element is still the weakest link in InfoSec (Ernst & Young, 2014; Delloitte, 2013; SANS, 2013). The understanding of the human element could assist in defining the security metrics and awareness strategy. The Global Security survey by PWC (2014) confirms that the human aspect of security is the major risk. The same company in 2013 suggested three means that could be used to improve employee awareness as mentioned here:

- Attitudes and Perceptions - beliefs and opinions regarding the value and urgency of information security
- Behaviour - action taken to mitigate Information Security risk
- Knowledge, Skills and Abilities - insight into information security policies, procedures, and controls, roles/ responsibilities and business impact

Awareness, skills and abilities build perceptions and attitudes, which influence behavior and, in turn, consistent behavior can influence the overall security landscape for the organization. Figure 1 shows how these three factors influence the overall information security. Understanding the relationship of the human factors of InfoSec could help in the drawing up of the metric as it informs the relationship.
Figure 1: Security awareness impact on other security aspects

Security threats until 2016 have among them mobile devices as a way of penetrating enterprise security (Durbin, Steve; Olasvsrud, Thor, 2014). The reason for this is that: “the rapid development cycle and lack of security considerations around mobile apps make them a prime target for cybercriminals and hackers seeking a way into the enterprise” (Durbin, 2014). Nowadays, most people in the community can afford cell phones (smart phones, tablet PCs and other mobile devices) and as such, are bound to use them for e-commerce. Since the security on these devices is weak more hacktivism and malicious software will threaten InfoSec.

The Vision 2030 for Namibia has set a target to make available the latest, most affordable, modern and adequate ICT infrastructure to facilitate economic development and competitiveness through innovation, research and development from the current level of 5.5 to 6.0 by 2017 (NDP4 page 77-8). The aim is to make Namibia a knowledge-based society by 2030 through reducing the digital divide between communities by ensuring the availability of broadband Internet in rural communities. NDP4: ICT provides fast access to information, which is a prerequisite for literacy and knowledge creation. These technologies are the modes of delivery for information economy (Government of Namibia, 2012).

Owing to affordability business processes will be conducted using smartphones or mobile devices (Durbin, 2014). These devices have a reputation of not being very secure, which presents an easier way for cyber criminals to get access into the enterprise by using them. The initiative to reduce the digital bridge and to enhance communication can also result in more InfoSec breaches. As the use of technology improves, precautions need to be taken to secure the beneficiaries.
Durbin and Olasvsrud (2014) recommend the incorporation of user devices into existing standards for access management, and that one should begin to promote education and awareness of BYOx (Bring Your Own Anything) risk in innovative ways.

Security Threats
An information security threat is an object that has potential to endanger information by exploiting vulnerabilities (Whitman & Mattord, 2011; Stallings, 2007). Table 1 summarizes threats to InfoSec

<table>
<thead>
<tr>
<th>Acts of human error or failure</th>
<th>Mistakes or accidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Espionage or trespass</td>
<td>Unauthorized access or data collection</td>
</tr>
<tr>
<td>Information extortion</td>
<td>Blackmail or disclosure</td>
</tr>
<tr>
<td>Software attacks</td>
<td>Viruses, Denial of service (DoS)</td>
</tr>
</tbody>
</table>

Table 1: Common threats to InfoSec

If users are to protect themselves fully from these threats they need to be knowledgeable about them. A study carried out by Huang, Rau and Salvendy (2007) concluded that perceptions of information security threats could be described by means of six factors, namely: knowledge, impact, severity, controllability, possibility and awareness. Awareness is the beginning of knowledge. In order to educate users about security there is a need to raise their awareness first. The learning continuum presented by NIST 800-16 shows that awareness should be attained before training, as it prepares users for training by altering attitudes to realize the significance of security and the penalties of its failure (1998). It is therefore very important to address the root of the security challenges by ensuring that users are aware of threats before equipping them with the skills to protect themselves.

Security awareness trends
Security awareness refers to sharing information by educating and training users about risks to data, especially risks to the confidentiality, integrity, or availability of data, and about knowing what to do to protect data (Peltier, 2005). Companies worldwide are integrating security awareness programs in their business process to reduce the risk of losing information (PWC, 2014). Much has been said about how to measure the success of an awareness program; however, it is important for every organisation to identify their unique measures as well as other factors such as organizational culture and environmental influence awareness.

For effective evaluation of security risk, metrics for a security awareness baseline should be identified. According to Hayden (2010) “Security metrics should be about choosing the best methods to determine what you need to know about security so that you can understand and improve your operational processes, within the resource constraints you face” The research focuses on identifying metrics that can be used to measure the impact of security awareness on user behaviour and information security.

Awareness will empower users to make the right choices (Navarro, 2007). Security can be assessed by answering the following questions:
Does the organization have security policies enforced?
Do employees know the security policies?
What are the practices and technologies in place that can help to detect a security breach?
Do employees know what to do if they detect a security violation?

Ernst & Young carried out a survey in 2013 on emerging technologies and trends and found out that successful security needs improvement, expansion and innovation in awareness programs in order to foster more proactive behaviour than reactive behaviour among users. Their survey results showed that respondents were more confident in the capabilities of current technologies in use because they are familiar with and confident of their capabilities. Organisations were cited as tending to place more importance on current technology rather than on emerging or future trends. This leaves the organisations unprepared to cope with the rapid changes in the IT field, hence poor proactive awareness programs (Ernst & Young, 2013; PWC 2014).

In a similar study by PWC it was found that cloud computing and BYOD are being implemented before being secured (2014). Such strides in technology are driven by advanced technical people and, as such, it would be expected that such issues should not be there; however, human behaviour is always playing a pivotal role in the success of security. According to Gary Loveland, a new model of InfoSec, motivated by knowledge of threats, assets, and the motives and targets of potential adversaries, is necessary to address current security challenges (PWC, 2014). Since security implementation is through policies it is necessary to define what a policy is. The next section will focus on that.

Security Policies
“A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area.” (SANS, n.d.)

They are perceived as the main means by which organisations officially set out their position concerning information security activities (Brotby & Hinson, 2013). Properly implemented, policies can mitigate threats especially those that are due to human aspects. As they address user behaviour, it is therefore important that they are specific and understandable. Since policies are point specific, it means that an organisation can have several policies to address their diverse ICT needs.

Security awareness approach
Survey data collected from a case site was analysed qualitatively, based on the findings that emerged. According to Yin (2009); Bhattacherjee (2012); Crinson and Leontowitsch (2011) case study research is a detailed inquiry of an issue used to evaluate the authenticity of the problem and allows researchers to gather realistic data of the phenomenon being investigated in social and behavioral scientific research.
Case site
A case study of the Polytechnic of Namibia (an academic institution in Namibia) was used for this paper. The Institution is located in the capital city of the nation, Windhoek. It has a student enrolment of 13400 per annum and employs 670 full-time staff. Every staff member has a desktop or personal computer (PC) and/or laptop allocated to him/her for daily work. The student laboratories and library are equipped with PCs, which are used for practical sessions as well as for information search on the internet and on e-library resources.

Materials and methods
A purposive, non-probabilistic method of sampling was used, targeting the sample population of staff members and aiming for a minimum of 30 responses.

Qualitative data analysis was used.

We therefore looked at the policing of and adherence to policies, as well as at security awareness.

The data gathered were classified according to exhibited patterns or characteristics, to allow for effective analysis. The classification was based on research aims and objectives. After classification of the data, we established connections among different categories.

The categories form the concepts or variables for the formulation of the theoretical framework, and for the relationships that form the connections. Meanings were logically inferred from literature. Description, contextualization, classification, processing and linking of gathered data were adopted.

Procedure
A survey was conducted in order to understand the security awareness levels in the case site. The population (site) was purposefully chosen to show the diversity of users from different backgrounds and professions, who use similar security features to achieve different outcomes. Purposive sampling is useful for circumstances where there is need to study a targeted sample in minimal time and proportion is not the key aspect. It is the most appropriate for selecting cases that are very informative (Saunders et al., 2009). Information about the knowledge of end users of the security threats to which they are exposed when they connect to networks; awareness of computer security policies in the organisation; and behaviour towards security alerts was gathered.

The objectives of the study were presented to the respondents in a cover letter. Based on this information, they made a voluntary informed choice whether or not to participate in the survey. Thus, purposive and self-selecting sampling techniques were used. Self-selection involves the participant volunteering to take part in the research and data was collected from those who responded. The responses were treated anonymously and in a confidential manner, to ensure that no link could be made to the participants who responded, on publishing the findings.
An online survey was designed to collect data from a population of about 670 end users using E-surveys Pro. The survey tool was pre-tested with seven users, after which it was deployed to all population members by means of a broadcast email containing the link. The online survey is quick and inexpensive to administer. Furthermore, it saves time in analysis as the data can be analysed electronically using statistical tools.

Participant selection
The participants in this study comprised lecturers, administrators and other professionals who make up the university community. Participants were chosen for this qualitative experience evaluation because they possessed the common experience of avoiding the use of security features for one reason or the other. The institution has 670 full-time employees. The population was chosen in order to reflect a diversity of users from different backgrounds and professions, who use similar application programs for similar purposes to achieve different objectives. Students were not included as the study was aimed at reflecting on a typical work environment.

The respondent composition was representative of the university employee population and was spread across the different faculties and centers in the institution. Table 2 below presents the respondents' affiliations.

<table>
<thead>
<tr>
<th>Department</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>School of Information Technology</td>
<td>18</td>
</tr>
<tr>
<td>School Of Business Management</td>
<td>8</td>
</tr>
<tr>
<td>School of Communication, Media &amp; Legal Studies</td>
<td>2</td>
</tr>
<tr>
<td>School of Engineering</td>
<td>2</td>
</tr>
<tr>
<td>School of Natural resources</td>
<td>3</td>
</tr>
<tr>
<td>School of Health &amp; Applied Sciences</td>
<td>1</td>
</tr>
<tr>
<td>Bureau of Computer Services</td>
<td>2</td>
</tr>
<tr>
<td>Centre of Open and Long life Learning</td>
<td>4</td>
</tr>
<tr>
<td>Centre of Teaching and learning</td>
<td>1</td>
</tr>
<tr>
<td>Centre of entrepreneurial development</td>
<td>1</td>
</tr>
<tr>
<td>Registrar</td>
<td>1</td>
</tr>
<tr>
<td>Library</td>
<td>1</td>
</tr>
<tr>
<td>Auxiliary Services</td>
<td>1</td>
</tr>
<tr>
<td>Payroll, Finance and Accounting</td>
<td>3</td>
</tr>
<tr>
<td>Human Resources</td>
<td>2</td>
</tr>
<tr>
<td>Namibian German Logistics</td>
<td>1</td>
</tr>
<tr>
<td>Security (Campus Control)</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 2: Respondents affiliation

Data Analysis method
Responses from 53 participants who completed the survey out of 58 respondents were analysed for patterns that demonstrate how much the users think they know about information security. To gauge the security culture of the organisation, general security information was gathered. The information captured the understanding of security, threats and solutions, as well as whether the end users were implementing them or not. Then the

behaviour of end users with security feature/ technology and the reasons for the specific behaviour was assessed.

After this analysis, the results were used to develop security awareness metrics using the steps outlined in the next section. The data collected helped in understanding the security metrics required at PON.

**Security metric program development process**

Security metrics provide information about IT security including costs and risks (asset value, threat and vulnerability are elements of overall risk) and must be based on a rigorous approach for security measurements and applied understanding seeking information security (Hayden, 2010). Useful metrics reflect the degree to which security goals such as data confidentiality are being met and they drive actions taken to improve the overall security program of an organisation. They can also identify the risk levels of not implementing certain measures and can be used to raise the levels of awareness within the organisation (Payne, 2006). According to Hayden (2010) security is the result of human activity. Hence, in this study the focus was more on measuring the third element of risk—vulnerability. Facets of vulnerability include the degree of understanding of security issues among computer users. Based on the results presented in the previous section, metrics were developed using the Goal-Question method. For instance, the metric is policy awareness. The question asked is: to what extent do you know the following policies? The goal is to measure policy awareness level. The following are the 7 steps involved in developing a security metrics program and in this paper the focus was on the first three (Payne, 2006):

1. Define the metrics program objectives and goals (provide metrics that clearly communicate how user interaction with security can be improved. Goals: to base the metrics program on improving awareness within our organisation; to communicate effectively the metrics to all stake-holders, including end users)
2. Decide on which metrics to generate using either a framework, top-down or bottom-up approach to determine which metrics could be desirable to use. Start with goals, measurements to generate the metrics. The bottom up approach in Table 3 was adopted using the analysis of the survey results.

<table>
<thead>
<tr>
<th>Bottom-Up Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify measurements that can be collected for this process</td>
</tr>
<tr>
<td>Determine metrics that can be generated from the measurements</td>
</tr>
<tr>
<td>Determine the association between derived metrics and established objectives of the overall security program</td>
</tr>
<tr>
<td>To increase security policy, threat and solution awareness among end users</td>
</tr>
</tbody>
</table>

Table 3: Bottom-up approach adopted from Payne(2006)

3. Develop strategies for generating the metrics (How will the data be collected?- Source (antivirus logs, user surveys), method of collection (survey, log analysis), frequency of collection, data analysis techniques, metric generation)
4. Establish the benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it
7. Establish a formal program review/refinement cycle.

Findings and discussions

Security policies active in the organisation (Polytechnic of Namibia (PON))

The following policies exist in the case site:

1. Acceptable ICT use which is meant for all ICT users in the organisation. It is meant to spell out the tolerable use of computer equipment at PON to ensure that the infrastructure is protected from “risks including virus attacks, compromise of network systems and services, disclosure of confidential information and legal issues” (Polytechnic of Namibia, 2008).
2. Password Policy which defines a procedure for creating and protecting strong passwords, and the regularity of change.
3. Remote access, which is applicable to all users remotely accessing the PON network with either a PON-owned or personally-owned computer, laptop, workstation or Palm device. Used to connect to the PON network for work-related activities.
4. Virtual Private Network which specifies how to use Remote Access through IPsec or L2TP Virtual Private Network
5. (VPN) connections to the Polytechnic of Namibia (PON) corporate network.
6. Wireless communication which forbids connecting to the Polytechnic of Namibia (PON) networks through unsecured wireless communication mechanisms and stipulates that access can only be granted by the ICT department.

All these policies are really good, but does the implementation create the right atmosphere? Security policies are hardly known to the users, and therefore not used as shown in Table 4. Using risk factor assignment to questions; no knowledge of security policies presents a high risk factor for InfoSec and the higher the knowledge thereof the low the risk. Findings reflect:

| To what extent do you know these policies? (1 is not at all and 5 is very well) |
|-----------------|---------|---------|---------|---------|---------|
|                 |        | 1       | 2       | 3       | 4       | 5       | Response Total |
| Password        |        | 11      | 2       | 11      | 12      | 15      | 51             |
| Wireless        |        | 14      | 9       | 14      | 7       | 7       | 51             |
| General computer usage |   | 13      | 4       | 14      | 9       | 11      | 51             |
| Internet        |        | 14      | 4       | 9       | 12      | 12      | 51             |

Table 4: Typical question

Response 1 is a very high risk factor (rated at 5) and 5 is the lowest risk factor (rated at 1). Generally the risk of policy knowledge is moderate to significant as the respondents are not knowledgeable of policies in the organization. According to practical lecturers and the technicians orally interviewed, students do not have enough storage on campus servers.

and accessible PCs, coupled with the fact that their user accounts have mandatory user profiles. A mandatory user profile loses user information/data upon log off. This encourages the use of removable devices among staff and students as they share materials. Survey results reflect that 81% of the respondents use memory sticks to share information. Memory sticks and email are the main means of sharing information. Other methods such as network, Google docs and Dropbox are just not popular. Emails and memory sticks are well known for propagating the spread of viruses. As a consequence of this, infections are rife in their labs and propagate to the production network. The anti-virus logs analysed show an infection rate of 85 virus infections in every hundred cases of malicious detections; the remainder being Trojan horses.

Security Policy awareness

A low policy awareness ranging between 13% and 29% for the different policies is evident as presented in Figure 3. Figure 3 shows that of those who know about policies, 45% learnt about them from a colleague or friend. Some have never heard about the policies yet they use the policies very well.

![Figure 2: Where users learn about security policies](image)

Users are generally not educated with regard to the existence of the policies, and they generally do learn about them from inappropriate sources. The findings reflect that there is no adherence to the policies as shown by the behaviour when confronted with a computer-related problem. The official way is to seek help from the Computer Services, yet about 42% seek it from the most untrusted source of information such as the Internet, or a friend or colleague. The general computer usage policy states that all sensitive information should be encrypted; yet the survey shows that only 15% of the respondents use the facility. This finding is a significant risk to information security.

Security Policy usage
Of the 51 respondents, 31 (65%) know and follow the requirements of the policies as shown in Figure 4.

![Figure 3: Knowledge of policy requirements](image)

Section 4.2.2 of the Acceptable ICT use policy states that users must ensure the security of all passwords and that they are not to share accounts. The survey reveals that when confronted with a problem 40%, will disclose their passwords to the “support” personnel. The support can be offered telephonically or using remote desktop managers. They do not have any perception of the implications of disclosing their passwords. The risk associated with knowledge of policy requirements is moderate.

**Security awareness levels at PON**

There is no user to train users on information security as confirmed by 92% of the participants. However, some users are aware of some security aspects as shown by findings. Table 5 shows the responses from 53 participants to the question: Have you ever heard of the following? (Tick all that apply)

<table>
<thead>
<tr>
<th>Heard of</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td>50</td>
</tr>
<tr>
<td>Phishing</td>
<td>45</td>
</tr>
<tr>
<td>Spam</td>
<td>49</td>
</tr>
<tr>
<td>Spyware</td>
<td>41</td>
</tr>
<tr>
<td>Virus</td>
<td>48</td>
</tr>
<tr>
<td>Worm</td>
<td>41</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>16</td>
</tr>
</tbody>
</table>

*Table 5: Knowledge of security threats*

Generally, there is high security threat awareness even with no training. Using risk assignments, this shows that the security in the organisation is at low risk. Further enquiry shows that 23% of the same respondents do not know if they have been hacked or not, 57% do not know if they have been victims of social engineering as presented in Figure 5.
End users (71%) download and install from the unsafe internet. This can lead them to download malicious programs such as viruses, worms, Trojan horses, logic bombs and many others, which will alter and destroy their information asset if executed. Since most (87%) have administrative rights it is quite easy for the compromised computers to be used to propagate the destruction of information in the organisation.

There is evidence of poor information backup practices, with only 22% performing the task always. In the event of a cyber-attack this will be very detrimental. Every computer has an administrator password which is maintained by the technical team. However, when confronted with a problem the participants give away their passwords to supposed helpdesk personnel, even telephonically. This practice exposes them to social engineering attacks. In an academic institution a lot is at stake, including student records. Summing up the findings there is moderate to significant risk posed by the awareness levels on information security.

Security metrics vs awareness

Based on the findings there is a need to develop and implement a security awareness program in the case site. Currently, the organisation is at level 1 of the security awareness roadmap depicted in figure 6.

Figure 4: Have you been a victim of any of the threats?

Figure 5: Security awareness roadmap adopted from SANS (2012)
The stages of implementing a security awareness program involve establishing a baseline, acting and then evaluating the impact. The security awareness metrics for establishing the baseline using the Goal-Question-Method presented in Table 6 is proposed:

<table>
<thead>
<tr>
<th>Metric</th>
<th>What is measured</th>
<th>How it is measured</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness survey</td>
<td>Number of users who: know about security policies, use policies, violate policies, know about security threats, breaches and solutions</td>
<td>Survey</td>
<td>To what extend do users know/ understand or use security tools, features or policies?</td>
</tr>
<tr>
<td>User behavior</td>
<td>Number of users who behave negatively with security</td>
<td>Survey</td>
<td>What is the current status in the case site?</td>
</tr>
<tr>
<td>Computer infections</td>
<td>How many computers are infected?</td>
<td>Antivirus logs</td>
<td>Are the infections behavior related?</td>
</tr>
</tbody>
</table>

*Table 6: Security awareness metrics*

For one to be able to design effective security awareness there is a need to carry out an awareness survey to establish a baseline. The baseline will serve as a reference or comparison point for measuring the impact of awareness campaigns. It is important to know what computer users know already. The findings reflect the absence of user training. This is a direct measure of metric 1. The second metric from Table 6 is user behavior which should align to policy and best practices, the number of users behaving negatively can inform an organization on the need to draw up a security awareness plan. It is important to have an understanding of what users do on the ICT resources. Thirdly, there is a need to know the computer attacks that affect the users, the frequency and how they impact on information and technology usage. Analysis of antivirus and system logs can reflect on the most prevalent infections, the sources, when it occurred and the number of devices affected. The source of infection and propagation mechanisms of breaches can inform what needs to be changed in terms of behavior and know-how.

**Conclusion**

The analysis of the collected data established that the policy awareness levels in the site were very low posing moderate to significant security risk for the case site. There is a need for a security awareness program to be designed and implemented especially addressing policy issues first since policies are the basis for defining best practices for human behavior with security-related issues. The awareness levels informed the identification of security metrics that can be used to establish the baseline state of security in a tertiary institution with security policies but no security awareness programs in place. This research identified what users need to be aware of namely security threats; policies and how to implement them in order to minimise the risk of vulnerability to information security threats; solutions and best practices. These are key indicators of the security risk levels.

The metrics extend existing work on security awareness by providing a measurement scheme for the first and second levels of the awareness roadmap. Information security officers can make informed decisions on areas of priority for the organisation and can thereby focus their programs on high priority areas first. The overall effectiveness of

awareness intervention can be enumerated using suitable security awareness metrics after the implementation of the awareness program. In this paper it is argued that institutions of higher education can improve employee interaction with security features through security awareness programs which can be evaluated using well-defined security metrics as proposed. Security awareness, the number and frequency of computer infections as well as user behavior can be used to enumerate the baseline security in an environment. There is a need for developing a security awareness model that can be used to focus on critical security awareness aspects for improving user behavior with security. Future research will also focus on evaluating the applicability of these metrics to other environments other than academic instructions as security awareness is a global issue not confined to academia.

References


