Factors affecting user experience with security features: A case study of an academic institution in Namibia

Fungai Bhunu Shava
PhD I.T. student Nelson Mandela Metropolitan University
Lecturer Polytechnic of Namibia
Windhoek, Namibia
fbshava@polytechnic.edu.na

Professor Darelle Van Greunen
Faculty of Engineering, Built Enviroment and ICT, School of ICT, Institute for ICT Advancement, Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Darelle.vanGreunen@nmmu.ac.za

Abstract

The widespread use of personal computers and other devices based on Information and Communication Technology (ICT) for networking and communication via the Internet exposes the end users to cybercriminals. Security systems and security features that interact with users via alerts, dialogue boxes and action buttons (such as update notices and other warnings) are embedded in operating systems and application programs in order to protect electronic information. Human behaviour and attitudes towards security features determine the user experience during the implementation of Information Security. Cyber criminals are primarily targeting the human aspect of security, since end users are easier to manipulate. In order to effectively secure information, the fields of Usable security and User experience should be integrated in the design and use of security features. This paper presents the findings of an online survey carried out to investigate attitudes towards, behaviour with and experience of embedded security features among members of staff in a tertiary education institution. User experience was measured by enumerating general security awareness, policy awareness and implementation, as well as user behaviour and emotions associated with security interaction. This paper reports on the findings of this survey. The researchers envisage that the findings can lead to the practical development and implementation of a framework for secure user experience.

Keywords- user experience; user behaviour; security feature; end user application program.

I. INTRODUCTION

Technology is shaping global behaviour by dictating how players must behave in order to survive the information technology age. Almost every job and communication now depends on information technology and is carried out with the aid of some application programs. Advancements in both system design and communication technologies have presented an opportunity for all to be interconnected. More end users are now connected to the Internet, including cybercriminals. This is enabled by the use of a variety of devices, some of which are mobile devices. Computers are now an integral component in homes and businesses, including in academic institutions like the one that was studied. Due to readily available network access, Africa has realised high Internet connectivity, and has an increasing number of novice end users connected to the World Wide Web. Namibia is rated as having an Internet user growth rate of 6.9% from 2000 as reported in the 2010- 2011 period [1]. With the launching of the West Africa Cable System (WACS), it is anticipated that Internet connection rates will drop allowing more Namibians to connect. This poses a security concern for the nation as cyber criminals will also find it easier to connect and also they will be presented with easier targets. To protect the end user's information, End user application programs have built in security features which interact with users to protect their information. Information security protects individual and organisation security from cyber criminals.

This paper presents the findings of an online survey carried out to investigate attitudes towards, behaviour with and experience of embedded security features among members of staff in a tertiary education institution. User experience was measured by enumerating general security awareness, policy awareness and implementation, as well as user behaviour and emotions associated with security interaction. The structure of the paper will be: User experience, Usable security, Case study, results and discussion, recommendations and conclusion.

II. USER EXPERIENCE

A. Definition

User experience (UX) is an individual's perceptions and responses as a result of use or anticipated use of a product, system or service [2]. For our studies we will adopt the alternative definition by [3] which defines UX as:

"a consequence of a user's internal state (e.g. predispositions, expectations, needs, motivation, mood, etc.), the characteristics of the designed system (e.g. complexity, purpose, usability, functionality, etc.) and the context (or the environment) within which the interaction occurs (e.g.

978-1-4799-0808-0/13/$31.00 ©2013 IEEE

organisational/social setting, meaningfulness of the activity, voluntariness of use, etc.)".

It is a discipline that falls in the field of Human-computer Interaction (HCI). User experience design (UXD) focuses on the emotional aspects of human experience such as happiness, although it is closely related to User-Centered Design (UCD) methods, which target human performance enhancement [4]. Since user experience refers to the overall perceptions of end users (effectiveness, efficiency, emotional satisfaction, quality of relationship with service entity) as they interact with a product or service [5], it is important that the design focuses on embracing all these factors in the security features.

B. End user experience

End users' perception of application program quality is based on their experience of interaction, as well as on those application program qualities that give rise to effective use and pleasure [6]. In order to have the complete picture of end user experience, it is necessary to consider the user's characteristics (such as skills, background, personality, motives and cultural values), product qualities (usability, appeal, behaviour) and the environment in which the interaction takes place [7], [3].

C. Usage Factors

Herzog and Shahmehri [8] realised that program security has features that influence the behaviour of users towards the execution or implementation of such features. It is important that designers focus on how to affect the user in a positive way. Studies conducted by [9], [10] show that it is possible to realign security and usability with careful attention to UCD principles, and make security usable. The question is: what characteristics does an application program have and how do they affect the user? Also: what characteristics does a user have that influence their experience with security features? We can look at how the environment, security culture and duties of the application program user shape their emotions when confronted with a dialogue that requires them to act in a secure manner.

Hassenzahl [3] came up with a model of UX which describes the designer's as well as the user's perspectives of product features. A designer has an intended product character on development, and puts up guidelines for the user to follow in order to get the desired experience. However because the user has characteristics that shapes how they perceive the product, the actual product character they encounter is different from the intended, in turn this evokes different consequences. We need to evaluate the extent of positive or negative feelings that can be experienced by end users in a particular environment, during and after interaction with the product. We also need to explore and how that influences further usage [6]. The evaluation helps us to determine how the interaction with security features can be guided to ensure a "degree to which specified users can achieve actual usability, safety, and satisfaction in use in a specified context of use" [11].

In order to evaluate the effect of a program's security feature on UX, various criteria that influence the overall UX can be used. Some important aspects are security policies, usability (convenience, efficiency, understandable, visibility) [12] user knowledge of security threats and solution and/or mitigation strategies related to their application programs. Giovanni [13] states that end user behaviour is directly linked to emotional satisfaction. It is against these factors that the researchers designed a survey to capture information on users' awareness of ICT security policies, their knowledge of security threats and solutions, the feelings invoked by interaction with security features and the behaviour that results from the feeling.

III. USABLE SECURITY

Usable Security (USec) also known as HCI security is the field that deals with human issues and Information Security, focusing on the design of security that is usable. It is defined as "A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users" [2].

A. Characteristics

The characteristics of USec include learnability, understandability, operability, efficiency, effectiveness and user satisfaction [14], [5]. Furnell [10] Investigated desirable characteristics of security such as locatable, understandable, convenient and visible; and realised that too usable can mean easy to compromise. A need to establish a balance between usability and complexity therefore exits. Furnell [10] also noted that there is need for more to be done to understand users' needs and address them.

As far back as 2005, [9] identified that realigning security and usability with careful attention to user centered design principles, security and usability can be synergetic. This area falls under the fields of InfoSec and HCI. It is important that we examine human behaviour towards security in our quest to address problems associated with end user security. The field of HCI is concerned with the design, evaluation and implementation of interactive computing systems for human use. Literature has shown that the human element is now the key to breaking or securing the information system. To secure the information, the security features presented to the end users must be usable in a way that appeals to them.

Whitman and Mattord [15] define poor usability as the tendency of end users to always prefer the easier option, when confronted with a choice between the official way of doing a job and the easier unofficial way. For example, whenever a new program update is available, the computer will prompt the user to update through an alert but will include an option to ignore or cancel. Choosing 'yes' implies that there will be more choices to make in future, while choosing to ignore the prompt to update will require the user to only click once without any further prompting.

The work done so far has not addressed the issues influencing the security of end user experience while interacting with these features. Previous work has focused on ensuring that security features are designed to be usable. The number of breaches associated with poor usage or no usage of security features is on the rise. Efforts to provide technically robust security solutions are fruitless if the beneficiary is not able to use them. We have investigated the factors that

influence user experience with program security features, and propose the model at Figure 1 that can be used to address the missing link between usable program security and user experiences. Much has been done to realign security design with usability. However, a lot still needs to be done to enhance or cultivate a positive experience with usable security.

Yeratziotis *et al* [16] used usability criteria to evaluate two online health systems. The criterion included trust, ease of use, terminology, ease of learning, feedback, awareness, errors, help and documentation. Yeratziotis *et al* [16] concluded that designers require tools that assist them to improve USec, in light of the fact that users need usable features to assist them in effectively securing their information.

This article presents the factors that influence end users to behave in the manner which they do. Assuming that the application program designers are focusing on embedding usable security features, what is left is to ensure that the end users secure their own information as well as that of the organisation.

B. End user application programs

These are the application programs that end users employ to perform daily tasks on their computers. The most popular used application programs as documented by [12] are web browsers (Internet Explorer), email client (Outlook Express) and word processors (Microsoft Word). In another Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office were also identified as popular application programs [17].

C. Security and security features

End user application programs have embedded security features such as the update service, password options, permissions, encryption, sharing security and other program-specific features. In a survey by [12], it was found that 73% of respondents used passwords even though the operating system under study (Windows XP) has logon as a security feature. Furthermore users are supposed to use passwords for online activities and to protect their information.

End users make use of application programs to access desired services on their devices and on the Web. Application programs have thus become the most used software in the information technology (IT) age, presenting cybercriminals with yet another means of accessing and manipulating user information [15], [17]. Software developers have embedded security features and components in end user application programs, in order to interact with end user to protect their information [12]. However, many end users regard security as an administrative function that should be handled by IT experts. As such they usually ignore security-related responsibilities, due to the complex nature of security and the fact that it is not perceived to be the user's duty [8].

IV. CASE STUDY

A case study approach was followed based on the approaches defined by [18], [19], [20]. According to these authors 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 behavioural scientific research.

A. Academic Institution

For the purpose of this research, a case study of the Polytechnic of Namibia (academic institution in Namibia) was conducted. The Institution is located in the nation's capital city 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 them for their 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. Each PC has a Windows or Ubuntu operating system installed for the daily business activities. Laboratories mainly use Windows, although in some departments Centos, Ubuntu, or MAC OS are used. Typical application software includes Microsoft Office, Internet browsers, integrated tertiary system (ITS), document readers (Acrobat), anti-virus software (Kaspersky lab), and email clients (mainly Thunderbird).

B. Materials and methods

An exploratory case study design was used as it allows researchers to gather holistic characteristics of real occurrences, such as group behaviours, within a population [18]. A purposive, non-probabilistic method of sampling was

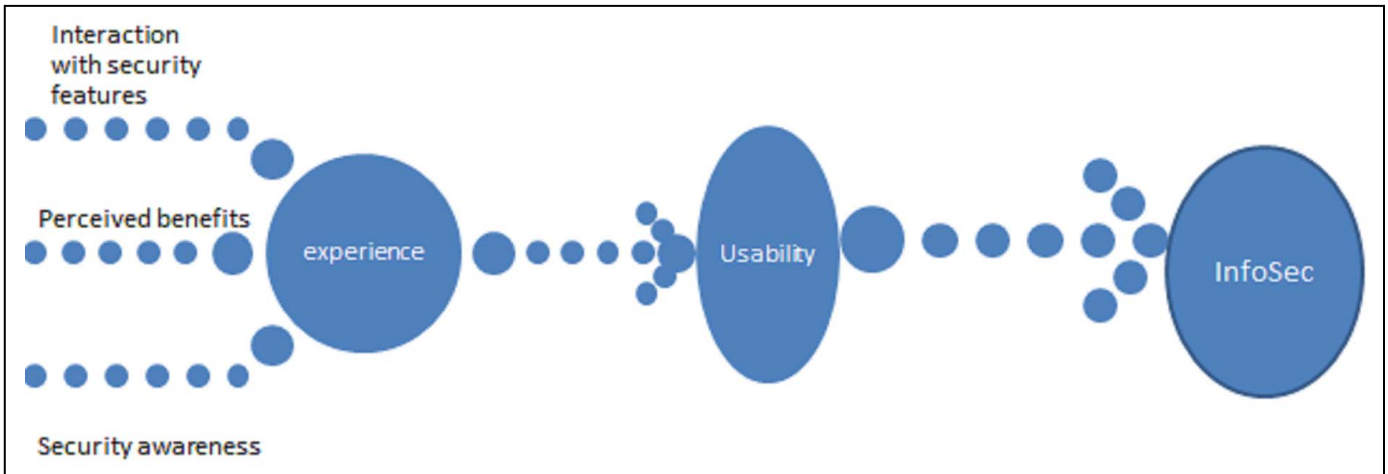

Figure 1: UX with security interactions

used, targeting the sample population staff members and aiming for a minimum of 30 responses. Qualitative data analysis was used. It requires rigorous analysis of the data, and a sample of 30 is therefore sufficient [21].

The study area was unambiguously described in the context of the case, as well as in terms of the objectives and actions to be taken [22]. The context in this case is shaped by the organisational security culture and support mechanisms that are in place. The researchers therefore looked at policing of and adherence to policies, as well as at security awareness.

The data that were 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, contextualisation, classification, processing and linking of gathered data were adopted.

C. *Procedure*

A survey was conducted in order to understand how the community handles security issues related to electronic information. In order to get an overall understanding of Information Security problems resulting from inadequate end user support, we gathered information about: end users' knowledge of the security threats to which they are exposed when they connect to networks; awareness of computer security policies in the organisation; experiences with security interaction; security technology/solutions usage among the community members; the application programs used for primary tasks at work/job; knowledge of security features embedded in application programs and operating systems; and behaviour towards security alerts.

An example of a question which was asked is shown in Figure 2. The end users would tick an appropriate level of knowledge for a policy in place.

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. The responses were treated anonymously and in a confidential manner, thus ensuring that upon reporting or publishing no link could be made to the population studied.

3. To what extent do you know these policies? (1 is not at all and 5 is very well)

	1	2	3	4	5
Password					
Wireless					
Internet					
General Computer usage					

Figure 2: Sample question

Semi structured interviews were carried out with 5 technical and 5 non-technical employees, in order to gain an understanding of the nature of the representatives of the population. Questions were open- ended so as to allow respondents to provide us with an insight into the situation. For further analysis, 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. It furthermore saves time in analysis as the data can be electronically analysed using statistical tools.

D. *Participant selection*

The participants in this research comprised of lecturers, administrators and other professionals who make up the university community. 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 composition of employees in organisation.

Out of the 53 respondents who completed the survey, 23 were female and 30 were male hence there was no gender bias. The respondent composition was representative of the university employee population, and spreading across the different faculties and centres in the institution.

E. *Data Analysis method*

Responses from a sample of respondents (53) were analysed for patterns that demonstrate how the users think and feel about embedded security features in the application programs that they use. After this analysis, we recommended mechanisms to ensure positive experiences for users while using the security features.

To evaluate UX we followed a hierarchical approach described by [13] which presents three stages, namely:

- Using general knowledge to provide a basic sense of end user program security awareness and usage;
- Understanding user behaviour to determine what users are doing and where a problem exists; and
- Influencing users by determining if a security feature is compelling through measuring the emotion associated with the feature.

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. We then assessed the behaviour of end users with security feature/ technology and the reasons for the specific behaviour. In order to fully comprehend the situation, the emotions of users associated with their interactions were also analysed.

V. Results and Discussion

A. Overview

The results are based on an inductive analysis of: security threats and solution awareness; user behaviour while interacting with security features; user attitudes and feelings towards security and the security policies that are in place. The interpretations are supported by extracts of actual responses.

A critical review of the literature has established that Information Security problems are largely due to a user's behaviour towards security features and perceptions of program security.

The survey findings indicate that many factors such as a lack of knowledge, awareness, prioritisation of work targets and misconception of security threats affect the experience of the end user with security. This experience in turn influences the tendency not to secure information. The following sections present results according to the sections of the questionnaire.

1. Systems Implemented

Table 1 shows that in our study population, the computer is mainly used as a tool for communication, for this task Thunderbird and Pronto Webmail are implemented. A variety of tools are used for research varying for the different disciplines and individual preferences. For Internet browsing several browsers are implemented including the default Windows browser Internet Explorer, Mozilla Firefox, Opera and Google Chrome. ELearning is implemented using Moodle and library services are electronic. Organisational Administration at all levels is implemented on the Integrated Tertiary system (ITS). The application programs used are mainly Microsoft products and open source software.

TABLE 1: Primary use of the computer

	% Always	% Sometime	% Not At All
Communication	87	13	0
Research	85	15	0
Teaching	57	38	4
Administration	51	47	2
Internet Browsing	83	17	0
Internet Banking	53	30	17
Downloads	40	34	26
Music, Skype, Games	17	51	32
Other	17	47	36

TABLE 2: Percentage Program Usage

	% Always	%Sometimes	% Not at all
Word processor	86	10	4
SpreadSheets	62	36	2
Presentation	62	36	2
Graphics	20	56	24
Project management	4	30	66
Document readers	50	28	22
Database management	18	42	40
Email	100	0	0
Web browsers	92	6	2
ITS	68	30	2
Other	26	52	22

2. Frequently used Application Programs

The most popular application programs are email clients which are used by 100% of respondents, followed by Web browsers at 92%, and word processors at 86%. ITS is used by 68% of respondents, followed by spread sheets and presentation software both at 62%. The document readers are used by 50% of the respondents, whilst the remaining programs are seldom used, as is shown in Table 2. The findings favourably compare with those articulated by [12], [17].

A diversity of email clients are in use, which is contrary to the expectation. The organisation under study uses CommuniGate pro (Pronto webmail) and Thunderbird as email clients. Findings indicate the use of several other email clients including Windows Live mail. Nine per cent of respondents selected other email clients and specified Pronto, which implies that there are 17 respondents (35%) using CommuniGate. Sixty-five per cent of respondents do not know that they use Pronto on a daily basis.

B. Factors

This section presents the findings about the factors which were studied.

1. Knowledge of security threats

The users are generally aware of the Information Security threats to which they are exposed., The survey showed awareness as high as 94% for hacking and as low as 30% for social engineering, other threats such as phishing, spam, spyware, viruses and worms were in the range of 74% to 92%.

However, only 13% of the respondents knew that they had been hacked, 24% were not sure and the remaining 63% knew they had not been hacked. Hacking is the act of gaining access to electronic information illegally [15]. It is quite likely that they do not understand how hacking is carried out, and that they can therefore not detect it. Of the 92% who are aware of what spam is, 64% knew that they have been victims thereof. The same trend is observed for all the other threats.

Further enquiry showed that 68% of the users were aware that their email programs handle spam. With this level of awareness, it is tempting to assume that they know how to handle their emails. However, 44% would open emails from unfamiliar sources and 29% opens all attachments that they receive.

Despite the fact that passwords are one of the most used security methods, and that users (over 70%) know how to implement them, 40% of users will disclose their passwords to the "support" personnel when confronted with a problem. Support is in these cases offered telephonically or via remote desktop managers. Users do not have a perception of the implications of disclosing their passwords. This indicates that there is no user training on Information Security, as is confirmed by 92% of the participants.

2. Security Policy awareness

Policy awareness is the key to successful implementation of security systems, in this study at most 29% of the participants know of the policies that exist in the organisation. Twenty-nine percent know about the password policy, followed by 23% of respondents that are aware of the Internet policy. The general computer usage policy is known by 21% of the sample population, and only 13% have knowledge of the wireless policy. Ironically, every staff member has a computer for their work, and all academic staff also have a laptop that connects both to the wired and wireless networks in the organisation. Out of those who know about policies, 45% learnt about them from the Rights office and the rest from a colleague or friend. These results show that users are not aware of the existence and proper usage of policies, and that the application thereof is hence not executed. User behaviour further indicates that there is no adherence to policies when users are confronted with computer-related problems. The official process is to seek help from Computer Services. However, about 42% of users seek help from the most untrusted sources of information such as the Internet, friends or colleagues. The general computer usage policy states that all sensitive information should be encrypted; however, the survey shows that only 15% of the respondents use the facility.

3. User experience with security interaction

The end users acknowledge that they receive security alerts and that they appreciate receiving system feedback. Security features from the point of view of the designers are meant to be usable. However, 63% of respondents have negative feelings with respect to notifications, especially when they are required to act on them (58%). Figure 3 shows some of the feelings that they experience with these interactions (such as disruptive, irritating and annoying).

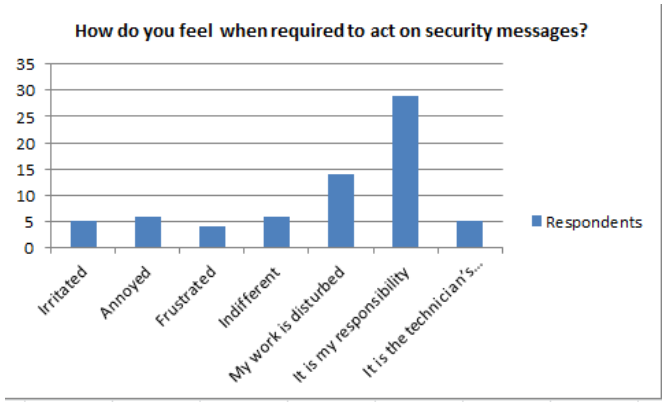

Figure 3: User feelings torwards acting on security messages

4. Security technology/Solution Usage

Anti-virus programs and passwords are the most used protection mechanisms with a prevalence of 72%, followed by firewalls. Updates are only implemented by 34% of respondents, which means that systems are left vulnerable to current and new attacks targeting known vulnerabilities. On further enquiry on users perform their updates, 70% of users identify with auto updates. The most shocking realisation is the fact that end users do not back up their information, with only 23% doing it.

The findings show that 46% of the participants configure security options. However, 68% are knowledgeable of the existence of spam filters in their email programs, possibly centrally configured for them by the system administrators. Other features such as encryption mechanisms for emails and files (digital signature, certificates same status) are rarely used. The security features interact with users through alerts, warnings and dialogue boxes in order to protect their information. A comparable survey carried out in 2006 also shows disturbing low usage of security technologies [12].

5. Embedded security feature knowledge

Only 46% of respondents have configured security options in their application programs. The idea of encrypting the information that is sent out via emails is virtually unknown, with only 4% using this feature. Embedded security is not being used as often as is necessary, and the absence thereof is making users an easy target for cybercriminals.

6. Behaviour towards security interactions

User behaviour is influenced by many factors such as lack of knowledge, prioritisation of their work targets and misconception of security threats [8]. The survey has confirmed the same facts. The majority of users make informed decisions (i.e. they actually read the screen before making a choice).

However, 18% ignore such information or just click in order to get rid of the message. When it comes to passwords, users seem to be more careful, although they are still susceptible to social engineering attacks. Users easily trust

anyone who claims to be technical support, with their login credentials (40% of respondents). They are cautious about email attachments, although they do trust emails from unknown sources.

When confronted with a computer problem, end users trust the insecure Internet (29% of respondents) for help, while 12.5% of respondents trust their colleagues to offer a solution. This exposes them to internal threats as well as to hackers. End users generally do not update their application programs as often as required with 27% of respondents doing it often, 53% when prompted by the software or technician, and 18.5% sometimes or never.

About 8% of respondents disable security programs from running on their PC and 17% disable alerts, but that the majority of respondents allow such application programs to run. Those who disable alerts do so because they feel negative about them. They feel irritated, annoyed, frustrated, or indifferent. Respondents also feel that their work is disrupted, or that it is the technician's responsibility to deal with security alerts. However, even among those who claim that it is their responsibility to look after security, there are some users who disable the alerts. This contradiction indicates that there is no alignment of behaviour to feelings (see Table 3).

There are mixed feelings about Web sensing, which manifests as a message that notifies the user that the page they are trying to access has been blocked by the organisation. Most respondents will navigate away from the site and do nothing about it. A few would contact the Webmaster. The patterns show that they are aware of restrictions to visit certain sites. If access to a genuine business related website is restricted, they act on it. However, the majority feels that it is appropriate for organisations to block some sites.

Another concern is the fact that many end users allow add-ons from the Internet to run on their computers, coupled with the fact that most of them have administrative rights (86% of respondents) on their machines. This poses a great security risk. Viruses and other malicious software can be executed remotely on their machines. Respondents download and install software from the Internet without making use of secure connections. Sixty per cent of respondents trust browser auto completion. This action might unknowingly lead them to a hacker's site.

7. Technology Acceptance

End users accept the use of a computer as a tool for accomplishing their daily tasks. However, they do not trust technicians with their information. Despite their comfort with technology they do not trust updates or new versions because it takes a lot of time to learn, because it moves them away from their comfort zone, or because of a fear of the unknown. However, some respondents are indifferent and will do as asked when prompted to update.

TABLE 3: FEELING ABOUT NOTIFICATIONS AND ERROR HANDLING

		Feelings about notifications						
		Irritated	Annoyed	Frustrated	Indifferent	Work is disturbed	My responsibility	Technician's responsibility
Alert Disabling	Yes	8	8	8	8	25	17	25
	No	7	9	5	9	19	47	4

C. *Discussion*

The results show that users are not trained with respect to security threats, solutions and secure behaviour while using information and communication technologies (ICT) to do their work. The organisation has policies in place to govern user behaviour with respect to ICT. However, end users have a low awareness of the existence of security policies and violate them by means of their behaviour. A large number of the participants download and install software programs from the Internet as they wish.

The results outlined above have several implications for Information Security. Considering the fact that all users have at least one computer connected to the Internet for their job, it is very important that all facets of Information Security [23] are addressed. However, due to lack of end user training, policies are violated exposing the participants to hacking attacks. End users (71% of respondents) 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 that will alter and destroy their information asset if executed. Since most users (87% of respondents) have administrative rights, it is quite easy for the compromised computers to be used to propagate the destruction of information in the organisation. The application programs that are most popularly used in the case site are rated as the most vulnerable by security experts [17]. This means that, with the human as the known weak link, attacks can be launched against the site via these application programs. There is evidence of poor information backup practices, with only 22% of respondents that are always performing this task. In the event of a cyber-attack, this would be very detrimental. Every computer has a super administrator password that is maintained by the technical team. However, when confronted with a problem, the participants give away their passwords to supposed helpdesk personnel. This is even done telephonically. This practice exposes users to social engineering attacks. In an academic institution a lot of sensitive information is at stake, including student records.

Poor security-related decisions and behaviour with an overall negative experience with Information Security are common, leaving application programs vulnerable to exploitation by cyber criminals.

VI. RECOMMENDATIONS

As interventions we recommend user training on computer security, ensuring that security policies are in place as well as the promotion of security-conscious behaviour.

Improving information security means improving the users' attitudes towards security features in the application programs that they use for their work. In order to improve the user experience with security features, users must be aware of security threats and solutions; they must know the benefits of using the features and must interact with the security features as required of them.

We recommend the UX model at Figure 1 with security awareness as the basis of feelings. Feelings shape attitudes and perceptions, which in turn influence behaviour. Negative behaviour with respect to security features will result in a negative experience with technology, and hence result in insecurity. This means that the user does not find the application programs usable for the job, resulting in information loss and/or compromise. Users will only be able to interact with embedded features if they feel good about it (the security will be usable).

VII. CONCLUSION

The research has highlighted problems that face end users while using computers to process, store and transmit personal or organisational information. The findings reflect a scenario in which there is a support mechanism from the organisation. It can be inferred that in scenarios where individuals are not supported, they experience more negative encounters with security. Based on the findings it is necessary to develop a framework for secure user experiences. The framework will ensure that users correctly interact while having a positive experience with built-in security features.

REFERENCES

[1] Statistics, Internet World, Internet statistics usage : the Big picture. Inrernet WorldStats. Available http://www.internetworldstats.com/stats.htm , 2011.

[2] A. Herzog, & Shahmehri, N. User Help Techniques for usable security. ACM(1-59593-635-6/07/0003), 2007.

[3] A. Hanudin,, and T. Ramayah, (EJISDC (2010) 41, 2, 1-15). SMS banking: explaining the effects of attitude, social norms and perceived security and privacy. The Electronic Journal on Information Systems in Developing Countries 41(2), pp 1-15. Retrieved from http://www.ejisdc.org/ojs2/index.php/ejisdc/article/viewFile/638/315

[4] M. Cummings, Designing for interaction :*User experience. UX design What matters to interaction design Professionals*. CA, Silicon valley, USA: Uxmatters, 2008.

[5] ISO 9241-210. Ergonomics of Human System Interaction- Part 210, Human-Centred design for Interactive Systems, 2010.

[6] K. Schulze, and H. Krömker, A Framework to Measure User Experience of Interactive Online Products. *7th International Conference on Methods and Techniques in Behavioral Research*. Eindhoven, Netherlands: ACM. pp. 1-5, 2010.

[7] P. M. Desmet, and P. Hekkert, Framework of Product Experience. International Journal of Design, 1(1), pp. 57-66, 2007, March 30 .

[8] M. Hassenzahl and N. Tractinsky. User experience - a research agenda. Behaviour & Information Technology 25(2), 2006, March – April. pp. 91-97.

[9] L. F. Cranor, and S. Garfinkel, Security and usability: *Designing systems people can use*. Cambrige, USA: O'Reilly Media Inc, 2005.

[10] S. Furnell Usability versus complexity - striking the balance in end-user securityNetwork Security, 2010(12), pp. 13-17. doi:10.1016/s1353-4848 (10) 70147-1, 2010, December.

[11] P. Lew, L. Olsina, and L. Zhang, Integrating Quality, Quality in Use, Actual Usability and User Experience. 6th Central and Eastern European Software engineering Conference CEESECR. pp. 117-123,2010. Moscow, Russia: IEEE.

[12] S. M. Furnell, A. Jusoh, and D. Katsabas, The Challenges of understanding and using security: A survey of end-users, Computers and Security, 25, pp. 27-35, 2006.

[13] C. Giovanni, Top 10 Tools to Measure User Experience, 2012. Pragmatic Marketing, Inc.

[14] Nielsen Norman Group, Usability 101: Introduction to Usability, 2012, retrieved May 04,2012 from http://www.nngroup.com/articles/usability-101-introduction-to-usability/

[15] M. E. Whitman and H. Mattord, Principles of Information Security. USA: Thomson Course technology. 2011.

[16] A.Yeratziotis, D. van Greunen, and D. Pottas, Recommendations for Usable Security in Online Health Social Networks. IEEE. 978-1-4577-0208-2/11 pp. 220-226. 2011.

[17] SANS. Security prediction 2012 & 2013: The emerging security threat. SANS. Available http://www.sans.edu/research/security-laboratory/article/security-predict , 2011.

[18] R. K. Yin Case study Research : Design and Methods (4th ed., Vol. 5). London, UK: SAGE Inc.University Science, 2009.

[19] A. Bhattacherjee, Social Science Research:Principles, Methods, and Practices, 2nd ed. Florida: Global Text Project, 2012.

[20] I. Crinson and M. Leontowitsch, Public Health textbook: Qualitative methods. UK: PHAST (Public Health Action Support Team CIC). Retrieved from http://www.healthknowledge.org.uk/public-health-textbook/research-methods/1d-qualitative-methods , 2011.

[21] P. DePaulo, Sample size for qualitative research,. QUIRKS, 12, 2000.

[22] I. Dey, Qualitative data analysis: *A user-friendly guide for social scientists*, London: Taylor & Francis e-Library, 2005.

[23] M. Ciampa, Security+ Guide to Network Security Fundamentals, 3rd ed., Boston: Tomson Course Technology, 2011.