A User Awareness Model for averting Computer Threats

Fungai Bhunu Shava and Attlee M. Gamundani

***Abstract*— One of the major reasons why systems are susceptible to threats in many ways or the other is the lack of the know-how and a follow up system for the education rendered to users, who in most cases are the weakest point for any perpetrated system attacks. Security awareness should be viewed as a gyratory exercise, as the attackers of systems never cease to explore on better and easier ways to penetrate organisational systems. This paper presents a user awareness model based on a case study done in one of the corporate environments in Namibia. The proposed model is a product of the different key facets that are perceived to be detrimental to system security in any average organisational setup. One of the major contributions of the User Awareness Model (UAM) is a systematic and procedural assessment tool of the user practice towards computer systems security, which can be applied to any organisational environment with the flexible option to vary the combination of security needs variables.**

***Key Words*— Awareness, Model, Security, Threats, Users.**

I. INTRODUCTION

Computer security is the process of preventing detecting and recovering from unauthorized use of your computer [1]. It can also be defined as tools designed to safeguard data and deter attacks [2]. Acts of protecting the computer are carried out by a computer user.

Computer users are individuals or devices who use a computer system to perform some task. The users can be classified as procedures that trigger some action on the machine, an expert/technical user who develops, maintains or administers the system and an end user who uses applications running on the machine to do their work [3]. The human users have varying knowledge and appreciation of computer and are vulnerable to different breaches. For example developers are exposed to buffer overflows and other programming coding errors while end users can experience phishing, viruses, inconsistent errors, e.t.c. [3] For the purpose of this paper we will focus on the end user definition of the user.

In order to successfully protect the computer systems and information, the user should have an upper hand of managing and controlling the computer. Literature however still attests to the fact that most breaches are a result of Human Computer Interaction (HCI) issues [4], [5], [6]. According to [1], the fundamental dilemma to computer security is the security unaware user who has specific security needs but no security competence.

There are 5 key aspects to HCI and these are: Nature of HCI (N), Use and context of computers (U), Human Characteristics (H), Computer Systems and Interfaces architecture (C), Development process (D) and are all applied to Project Presentation and examinations (P) [7]. The human characteristic in security is still the major concern for the security officers in different organisations.

The human characteristics focus on User Experience, Interaction and behaviour, the relationship is depicted in Fig.1. Computer threats are usually propagated through desirable/ undesirable user behaviour. How can user behaviour be modelled for computer security? A common proverb states that knowledge is power. If users are knowledgeable of computer threats, security solutions and how to handle them, most of these issues will be minimised.

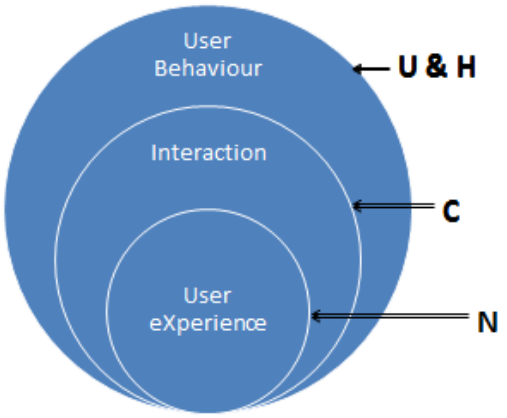

Figure 1: The Relationships of HCI aspects

Learning is a three stage activity made up of awareness, training and education [8], [9]. "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly" [10]. Before training of hands on skills and education for knowledge acquisition it is necessary to provide the elementary need "awareness". Awareness also features as one of the key security principles identified by Organization for Economic Cooperation and Development [11]. According to [12] security awareness offers the know-how of the significance of security within an organization; enlighten employees of their responsibilities, and expectations surrounding their responsibilities, in the fulfilment of information security necessities. It is also a source of direction around the implementation of a particular security function, as well as information about the security functions.

Raising User awareness is therefore a tool that can be used to enhance computer security [13]. Correct training can empower users to be the strongest security strength (Navarro, 2007). However security responsibilities are not the user's primary focus when they use the computer, hence it interferes [14].

Computer security can be modelled as a set of relationship between users and objects (operational policies) and its implementation in hardware and software components of the computer system. Security models focus on the implementation of security policies.

"A model is an abstract, conceptual construct that represents processes, variables, and relationships without providing specific guidance on or practices for

implementation" [15]. Of importance is to understand the construct we intend to come up with. In its simplest form a model presents relationships among variables and is technology independent [15]. On the other hand "A security model defines a method for implementing policy and technology" [16]. Our model will be independent of technology hence should be applied across different computer systems and security technologies. "Models provide guidance for the completion of work or the establishment of systems and refer to a representation of a real world phenomenon." [17].

The paper will focus on developing a user awareness model for improving computer security by focusing on the key elements of user awareness.

The paper will present computer threats, attacks, solutions, the case study where the research was conducted, the methodology followed to design the user awareness model, the user awareness model itself, the model review and conclusions.

II. COMPUTER THREATS

A threat is defined as a potential violation or breach of computer security by exploiting a weakness [2]. A computer threat is a violation of computer security. Examples of threats are unauthorized disclosure of information which violates the confidentiality goal of security, deception, disruption and usurpation [18], [19]. They can also be classified as interception, interruption, modification and fabrication [20]. When a threat is successfully carried out then it is an attack or security breach.

Social engineering (phishing), Hacking , Spam, Malicious code (viruses, trojan horses, web scripts, malware(adware, cookies, spyware), worms, botnets, zombies), Pharming, DoS, Spoofing ,War driving, Password cracking, Back/trap doors, Buffer overflows, Eavesdropping , Intrusion, Replay attacks and sniffing (penetration) are among the common threats to security.

Different threats target different aspects of security, to fully address security one needs to consider the technology, process and people issues. Since security is as strong as its weakest link, it is vital to address this link, which in this case has in recent years been identified as the human aspect [21], [22], [23]). As such it is important that we focus on those threats that target the human security.

Threats to the human aspects of security include: social engineering, phishing and these threats succeed in attacking the user mainly because, the users are not aware of how vulnerable they are and which mechanisms are at their disposal to protect themselves.

A. How are systems attacked?

When a threat is successfully carried out it becomes an attack [18]. Attacks can be active or passive. Active attacks modify the information, while passive attacks do not modify the information. The main categories of attacks on computer systems include Malicious Code (Viruses, Worms and Trojan Horses); Reconnaissance Attacks; Access Attacks; Denial of Service (DoS) Attacks and Cyber-attacks. Depending on the attack being propagated, the attack method will include social engineering, Intrusion and sniffing (penetration), war driving, code injection, DoS, Buffer overflows and Replay attacks. Eavesdropping and traffic analysis are examples of passive attacks [2],[19]

Security threats target security services which are meant to secure computer information. Security services include Confidentiality, Integrity, Availability, Access Control, Authorisation, Authentication, Non Repudiation and so on [2], [20].

Since security assumes multiple layers, the attacks are also directed to the different layers. Different authors present the security layers differently depending on the context; however all depict the products, people, policies and procedures [24]. [25] presented three layers of application security namely operational, tactical and strategic. The operational layer deals with User accounts and access rights, Password controls and Segregation of duties [25].The tactical layer deals with Security administration, IT risk management, Application patch management, Interface security and Audit logging and monitoring [25]. The outer layer is the strategic which deals with security policies and standards, user awareness, IT risk management framework and guidelines, IS governance metrics and reporting [25]. Operational cyber security risks are defined as operational risks to information and technology assets that have concerns impacting on the confidentiality, availability, or integrity of information [26].

The research focuses on the operational and tactical layer as the user is an element of this layer [24], [19], [25]). [26] present taxonomy of operational cyber security risks as follows: actions of people, systems and technology failures failed internal processes, and external events. The question is what are the critical security factors in play?

[27] identified knowledge of security awareness as one of the factors affecting information security as it can change user experience, perceptions, attitudes and behaviour with security features.

B. Which Solutions are being employed?

Security solutions are broadly classified as preventive, detective or reactive. Preventive solutions protect the information from being compromised. Detective solutions detect security violations that have occurred. Reactive security allows your information to be recovered from the damage perpetrated by the attacker.

To secure computer systems several solutions have been proposed and used for decades now. Classification of the solutions include: user centred design methods, information security governance and risk management, physical security, operation security, access controls cryptography.

The most popular solutions include: Secure channels, Firewalls, Backup, IDS/ IPS, Scanning, Access control, Cryptography, VPN, Certificates ad signatures, Antivirus, Disconnect from the Internet when Idle, Avoid following unknown Links, update all active programs, patching software, uninstall all inactive software [24].

Information security management forms the basis of an adequate prevention security program to protect an organization's information. Security management focuses

on technical, physical, and administrative controls required to fully provide confidentiality, integrity, and availability of information. Controls are established through policies, procedures, standards, baselines, and guidelines [28].

Security awareness is one of the Information security management practices for risk management which are used to minimize information threats and attacks by identifying, measuring, and controlling"[28]. The awareness roadmap follows five stages namely: no awareness program, compliance focused, promoting awareness and change, long term sustainment and metrics [23].

To evaluate the effectiveness of these security solutions, metrics to enumerate the effectiveness and usability of security exist. Security usability metrics include: visibility, aesthetic minimalist design, learnability and satisfaction [6].

The last five solutions focus on human behaviour as a means of addressing security threats. End users need to be knowledgeable of the risk of staying connected to the Internet while not using their system as well as how they can easily fall prey to cyber criminals by clicking on unknown links.

The third domain of the domain of the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) deals with information security governance and risk management.

Some organisations have designed and implemented security awareness programs for all their personnel.

C. Analysis of existing security solutions on threats

Technologies are designed to address specific security problem, there is no one size fit all. Even with the right solution, there is needed to be correctly applied by the end users for them to be effective. Users are usually challenged when it comes to understanding and applying these solutions when they are not aware of the risk they are exposed to, the implications of having inadequate security, the correct way to apply the technology to protect their systems.

III. THE CASE STUDY SETTING

A case study research was followed as it allows researchers to gather realistic data of the phenomenon being investigated in social and behavioural scientific research. It is a detailed inquiry of an issue used to evaluate the authenticity of the problem [29],[30].

A qualitative case study of an academic institution in Namibia's students from 5 faculties was conducted. The Institution is located in the Namibia's capital city Windhoek and has around 13400 students enrolled per annum. The students have access to computers in laboratories and the library.

A. Methods

For in-depth study a case site was purposefully selected for its diversity of participants which enables the researcher to have a general view of awareness across the institution. Stratified and convenience methods of purposeful sampling were used. Stratified demonstrates features of specific subcategories of the whole population being studied and enables comparisons between the different categories. Due to varying knowledge of computer systems and security issues there was a need to represent students from all faculties and look out for variations among the different fields of study. On the other hand convenience sampling allows for the first available participants in the strata to take part in the study. Students from Management (Accounting and finance; Economics), Human Sciences, Engineering, Information Technology and Natural Resources & Tourism were targeted aiming for a minimum of `10 responses from each faculty.

Data analysis was qualitative and requires rigour; therefore a sample of 25 is sufficient [31]. The data that were gathered were classified according to target questions or characteristics, to allow for effective analysis. The classification was based on research aims and objectives. After classification of the data, connections among different categories were established. The categories form the concepts or variables for the formulation of the model.

B. Procedure

A survey was carried out to understand the student security awareness levels in the case site. We gathered information about: students' knowledge of the security threats; awareness of computer security policies in the college and security technology/solutions usage among the students as well as the programs used.

The objectives of the study were presented to the respondents in the survey introduction. Students made a voluntary informed choice as to whether or not to participate in the survey. The responses were treated anonymously and confidentially.

Questions were closed so they were meant to assess the situation. The survey tool was pre-tested with 5 students, after which it was deployed to target participants.

C. Participant selection

Students from the five faculties were purposefully selected, as an equal representation of the faculties was required for comparison purposes.

D. Data Analysis

The data was categorised according to awareness element which were being investigated, namely security threats, security solutions, security policies and their faculty affiliation.

E. Results

Students from IT are aware of security threats and solutions compared to the other faculties. Engineering and Natural Resources & Tourism showed a good awareness level, however the same could not be said of the other two schools except on viruses and worms. The results reflected a very low awareness of phishing and social engineering in general. The two low areas are human related. When it comes to policies the wireless and general computer usage are very popular, this could be attributed to the college culture. Before any mobile device can be joined to the Campus Wi-Fi the student is required to read the policy and sign a consent form. All labs have a general computer rules and in order for the students to gain access they need to register with their lab technician for an account and

during this exercise they are required to read the general computer usage policy. This s also reflected in their knowledge of passwords as a security mechanism. However when it comes to email, network and ITS policies only IT students had an upper hand, which can be attributed to the nature of their studies. In a comparative study carried out by [27] among staff members in the case site the a similar trend was observed. Policies stipulate how users should behave or act with technology in the case site, however there is no sytematic awareness program being implemented. Beside the general computer usage and wireless policies which users learn about upon getting access to the resourses, the rest are not well publicised. There is need for developing and implementing a security awareness strategy. Development of the program is the first stage, therefore it is necessary to understand what needs to be addressed, come up with a model to follow which can be applied all the times iregardless of the security oficer in charge before cosidering **how** the awareness program can be implemented. The following section will present the process followed in designing the user awareness model for this context.

IV. DESIGNING THE USER AWARENESS MODEL

The model development will follow a three step level involving: identifying the variables through literature study and evaluation of existing models; identifying and explaining the relationships through analysis of survey results, and developing the model [32].

In this section an analysis of security awareness models will be presented. Most of the existing models in literature focus on evaluating security awareness/ or the programs used to attain the security levels [33], [34] as well as to provide an awareness process or roadmap [35], [23], [10] provides different models for developing awareness programs. There are models developed to measure awareness maturity [23].

All models presented by the different authors do not analyse user awareness on a granular level and are biased towards organisational security. Trends in ICT deployment have since shifted towards mobile devices; these devices are owned by individuals hence security is now at a personal level. BYOD integrates these personal devices and business activities hence personal and organisational threats are similarly integrated.

Extended general deterrence theory (GDT) model, behavioural intention model (BIM) and information security awareness (ISA) classification scheme closely relate to our study and the summarised analysis is presented in table 1, later on components of the proposed model are identified.

Table 1: Analysis of Models

Literature	What	When	Where	Why
The extended General Deterrence Theory model [36]	Security countermeasures Security policies; Security Education Training and Awareness (SETA) program and Computer monitoring Sanction perceptions	-	Organisation	To avert misuse
Classification scheme [37]	Security awareness classification	-	Organisation	To identify and classify unclear aspects of security awareness approaches. Role of IS stakeholders, Desirable outcome
Behavioural Intention Model [35]	Policy compliance Security culture	-	Organisation	to enhance information security culture promote acceptable information security behaviour

The extended GDT model by [36] presents the impact of user awareness of countermeasures on perceived intention and information misuse. They used severity of sanctions as an influencing factor on overal behaviour as well. The model presents what the user need to be aware of, in this case security policies; security education training and awareness (SETA) program and computer monitoring, why they need to be aware of these elements, in an organisation setup.

The BIM is a combination of best elements of three theories: theory of reasoned action (TRA) which deals with behaviour intention (BI) influences; protection motivation theory (PMT) which attest that behaviour intention is a result of perceived danger and impact; and behaviourism theory (BT) which states that behaviour change is evidence of learning and can be attained through conditioning [35]. The resultant BI of applying the 3 theories is a behaviour shift towards security compliance and positive security culture in organisations.

The ISA classification scheme by [37] presents six domains of security awareness which start with distinction of awareness, training and education; desirable outcome (objective of the awareness); evaluation approaches (metrics); process (organisation) or product aspects; role of IS stakeholders and conditions intervening to success.

The two models and the ISA scheme presented do not go beyond the organisation context and they make no reference to when the awareness can be applied or enumerated. Based on this analysis, identification of variable then follows.

The variables for the model are the constructs that need to be related in order to address user awareness. The dependant or criterion variable is what propels the research, in this case **user awareness**. The factors that influence it are the independent variables which were identified as **what**, **when**, **where** and **why**. The following section will discuss the independent variables in detail with reference to selected awareness models which closely relate to our work.

What do they (users) need to be aware of? The user needs to be aware of the security threats they are exposed to when they use computers, security solutions they can implement to protect their information, secure behaviour that is expected of them (their role) and the importance of the different types of security policies they need to adhere to for effective security. [34] Identified 3 elements that can be measured to give an overall security awareness level for organisation setups. The elements were constituted into a model. These elements are Knowledge (what the users know focusing on policies and passwords), Attitude (what they think/ perceptions about the aspect) and Behaviour what users do). The attitudes and behaviour will not be addressed in this paper.[PWC also]

When do they (users) need to apply the awareness? When they actively interact with their computers both offline and online, as well as when they leave their computers idle. Different threats operate in different modes, some need the user to execute an action while in some cases access to a running computer is sufficient for the attacker to carry out their actions.

Where do they usually attack? Do you know that your information is the target? Security attacker/ hackers can attack computers used at personal or business levels. The computers that connect to public networks are the most vulnerable, however even the protected ones are often exploited as well. There are attacks that target online (connected to the internet) and those that can attack offline machines. How?

Why do users need to be aware of computer security threats, solutions, behaviour and policies? In order for users to behave in ways that do not compromise security, prevent attacks on their information and ensure that they are always up to date.

V. THE USER AWARENESS MODEL (UAM)

A. The refined ingredients

As a sequel to section IV above, we will make the reader understand the specific ingredients we used in our model and may want to justify why we focused on such ingredients and exclude others, if we might have proposed to do so.

B. The key pillars of the User Awareness Model

Building the user awareness model, based on the sources and possible solutions to attacks and threats, the following are the key building blocks.

What? There is need to establish the sources of security points. At this stage, it is all about sensitising users on the threats and the policies designed or to be designed.

When? This level is trying to establish the conditions that attacks or threats could occur and require that users be aware of the safe practice to extend when using their various computing devices. This is a stage that explains why such practice where users leave their machine idle while connected to the computer; this is one of the practices that may cause passive attacks of their devices.

Where? The need to establish the necessary precautions to advance depending on the places users will be operating from or interacting with, is quite key. Considering workplaces for instance, they may have some level of security levels in place, like firewalls; in comparison public access points may not extend an equal security to data or device components, which increases the level of security risk.

Why? Users interact with security messages on their computers and are constantly required to make informed choices. Technology can protect systems, however users control the technology; therefore it is essential to raise user awareness in that regard [38], [39], PWC, [40]. Giving some explanation as to why users need to consider security practice as their main responsibility and taking care of their actions, will pave way to the broader appreciation of the security objectives. This will improve acceptance levels of policies, solutions and best practices [38], [41]. Research by [37] focused on these as desirable outcomes and roles of the information security stakeholders. Protection Motivation Theory (PMT) is well known for forecasting an individual's plan to employ defensive actions [42]. According to [35] Information security awareness and training impart knowledge in users and supports in encouraging protection.

C. *The User Awareness Model (UAM)*

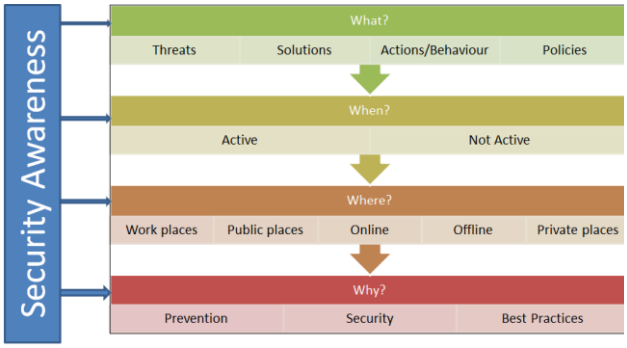

Figure 2.The User Awareness Model

VI. APPLICATION OF THE USER AWARENESS MODEL

The proposed user awareness model proposed in this paper follows a simple decision flow approach, by asking the right and critical questions, the awareness could be extended to the concerned parties in a security domain scenario. The users or devices that need to exercise security checks and applications will be equally equipped to validate the necessary pressure points. The four key questions that build the pillars of the proposed user awareness model (What? When? Where? and Why?), aid those concerned with security applications to ask the right questions and if they can avail the right solutions to such questions, they would have built a relatively strong security environment for their organisation or for personal protection.

We therefore propose a cascading flow of the model's application, which entail, if a what question is asked, we are likely to open the options to consider all the possible sources of threats and work around them. The when, question will give a high level view of the likely occurrences of the identified threats at that level. Considering the where level, there is a contextualisation of the possible security concerns to be weary of.

Precisely, the proposed user awareness model is crafted on the simple premise that, if we can answer the key questions, we may have, as to what may cause security to be the primary responsibility, when do they need to exercise such responsibility, where they have to exercise such responsibility and why they need to exercise such responsibility. Such procedural security awareness plan may yield reasonable practical results, as users are motivated to consider every detail of security within their sphere of influence.

VII. A REVIEW OF THE USER AWARENESS MODEL

A technical review of the user awareness model will obviously point to the inability to spell the specific solutions that can be applied at each of the level of awareness that are depicted in this paper. We therefore recommend that, depending on the context in question, once users are sensitised on the key pressure points to be on the lookout for, the relevant technical prevention solutions be put in place. An awareness exercise is not security itself, but clears the way for security implementation, sustenance and continual improvement.

This simplified model is flexible for application across main domains and can be fine-tuned to suit particular organisational setups and functional areas that may require security awareness campaigns. We consider this model as a turnkey solution to security first level needs. If an organisation desire to extend an educational stature to its security needs, applying the four key pillars of the UAM model presented here, will ease up the planning and implementation process.

VIII. CONCLUSION & RECOMMENDATIONS

This paper tackled the challenge that faces many security strategies. Many security implementations overlook user awareness, which could be very vital in ensuring the organisational or individual security levels are heightened. Implementing and designing security policies without communicating to users, is normally a futile exercise.

Based on the proposed model (UAM), in this paper it is clear, that user awareness is not a once off exercise, at every stage of the security life cycle, the model could be consulted and applied accordingly. A pre-awareness and post awareness campaign when deciding on a security solution to implement could be extended.

We envisage this proposed model will provide a systematic and procedural way to assess the user practices towards computer systems security in organisations. The model can also be used to inform the development of relevant tools for measuring the impact of security awareness programs.

We recommend the need for validation of the model presented in Fig. 2, by experts in the field of computer and network security. Practical implementations on an experimental basis are highly encouraged as this is work in progress. We can only confirm the existence and practicality of a fine churned model after all the necessary model design and testing procedures have been executed to the latter.

ACKNOWLEDGMENT

We commend all those who participated during the research at the data gathering stage, as well as at the point of writing this paper. The time rendered to proof read this presentation by Mercy Bere is highly commendable.

REFERENCES

[1] D. Gollmann, "Computer Security," West Sussex, England: John Willey & Sons, Ltd, 2006.

[2] W. Stallings, "Network Security Essentials: Applications and Standards," 3rd ed. NJ: Pearson Education, Inc, 2007.

[3] F. Beisse, *A Guide to Computer User Support for Help Desk and Support Specialists* 3rd ed., Phoenix: Course Technology, 2004, ch1 pp. 1-36. Retrieved August 13, 2013, from http://ghc.edu/faculty/slloyd/CIS211/Chap1.pdf

[4] S. M. Furnell, A. Jusoh, & D. Katsabas, The Challenges of understanding and using security: A survey of end-users. Computers and Security, 25, 2005, pp. 27-35, Retrieved January 24, 2012, from www.elsevier.com/locate/cose

[5] A. Whitten, & J.D. Tygar. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," In L. Cranor, & G. Simson, *Security and usability: Designing secure systems that People can use*, O' Reilly,2005, pp 679-702.

[6] J. Johnston, J.H. Eloff, & L. Labuschagne, Security and human coputer interfaces. Computers & Security, 22(8) , 2003, pp. 675-684.

[7] T. T. Hewlett, R. Baecker, S. Card, T. Carey, J. Garsen, M. Mantei, W. Verplank. SIGCHI. New York: ACM,1992

[8] T. R. Peltier, Implementing an information security awareness program. Security Management Practices, 2005, pp 37-49.

[9] NIST. Building an Information Technology Security Training and Awareness Program. NIST Special Publication 800-50, 2003, pp. 1-70,

[10] NIST. NIST SP 800-16 – Information Technology Security Training Requirements: A Role- and Performance-Based Model. USA,1998

[11] OECD. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002. Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultur○eofsecurity.htm

[12] C-H. Chu, Security organization- theory & practice learning by practice. Pennsylvania, USA: Pennsylvania State university IST515,2008 Retrieved from https://online.ist.psu.edu/sites/ist515/files/.../106securityorganization.ppt

[13] F. P. Bresz. People—often the weakest link in security, but one of the best places to start. Journal of health care compliance, 6(4), 2004, pp 57 – 60.

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

[15] B. L. Tomhave, Alphabet Soup: Making Sense of Models,Frameworks, and Methodologies,2005 http://secureconsulting.net/papers-publications.html.

[16] H. F. Tipton, & M. Krause. *Information Security Management Handbook*. Auerbach Publications, 2007

[17] F. Shafique, & K. Mahmood. Model Development as a Research Tool: An Example of PAK-NISEA. Library Philosophy and Practice,2010 Retrieved from http://www.webpages.uidaho.edu/~mbolin/shafique-mahmood.htm

[18] W. Stalling & L. Brown. *Computer Security Principles and Practice*. Upper Saddle River, NJ: Pearson Prentice Hall, 2008

[19] M. E. Whitman, & H. Mattord. *Principles of Information Security*. USA: Thomson Course technology,2011.

[20] C. P. Pfleeger, & L. S. Pfleeger. *Security in Computing* 4th ed. New Jersey, USA: Pearson Education Inc, 2007

[21] Ernst & Young. Insights on governance, risk and compliance- Under cyber attack: EY's global information security survey 2013. Ernst & Young, 2013. Retrieved December 12, 2013, from www.ey.com/giss

[22] Deloitte. Blurring the Lines Information security in a world without boundaries. Technology. Deloitte Touche Tohmatsu Limited,2013. Retrieved February 6, 2014, from http://www.deloitte.com/assets/Dcom-Guam/Local%20Assets/Documents/Technology,%20Media%20and%20Telecommunications/Blurring%20the%20lines%202013%20TMT%20Global%20Security%20Study.pdf

[23] SANS. Security prediction 2012 & 2013 The emerging security threat. SANS, 2011. Retrieved February 24, 2012, from http://www.sans.edu/research/security-laboratory/article/security-predict2011

[24] M. Ciampa, *Security Awareness: Applying Practical Security in Your World*, 4th ed. Cengage Learning, 2014.

[25] A. Adaikkappam, "Application security controls: An audit perspective," ISACA, 6,1-7,2009.

[26] J. J. Cebula, & L. R Young. *A Taxonomy of Operational CyberSecurity Risks*. Software Engineering Institute. Carnegie Mellon. doi:Technote CMU/SEI-2010-TN-028,2010.

[27] F. Bhunu Shava, & D. van Greunen, Factors Affecting user experience with security features" A case study of an academic institution in Namibia. Information Security for South Africa (pp. 1-8). Johannesburg: IEEE, 2013. doi:10.1109/ISSA.2013.6641061

[28] S. Hernandez. *Official (ISC)^2 guide to the CISSP CBK*, 3rd ed. NW: Taylor Francis Group, 2013.

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

[30] R. K. Yin. *Case study Research: Design and Methods*, 4th ed., Vol. 5. London, UK: SAGE Inc, 2009.

[31] J. W. Creswell. *Qualitative inquiry and research design: Choosing among five approaches*, 2nd ed. Thousand Oaks: Sage Publications, 2007.

[32] U. Seckran, & R. Bougie, *Research methods for business: A skill Building Approach*, 5th ed. UK: John Wiley & Sons, 2009.

[33] B. Khan, K. S. Alghathbar, S. I. Nabi, & M. K. Khan. Effectiveness of Information Security awareness methods based on psychological theories. African Journal of Business Management, 5(26), 10862-10868. doi:10.5897/AJBM11.067,2011

[34] H. A. Kruger, & W. D. Kearney. A prototype for assessing information security awareness. Computers & Security, 25(4), 289 -296. doi:10.1016/j.cose.2006.02.008,2006

[35] T. Gundu. Towards an Information Security Awareness Process for Engineering SMEs in Emerging. Alice: Fort Hare University,2012. Retrieved April 27, 2013

[36] J. D'Arcy, A. Hovav, & D. Galletta. User awareness of security countermeasures and its impact on Information Systems misuse: A deterrence approach. InformationSystems Research, 1-20. doi:10.1287/isre 1070.0160, 2008.

[37] A. Tsohou, S. Kokolakis, M. Karyda, & E. Kiountouzis. Investigating information security awareness: research and practice gaps. Information Security Journal: A global perspective, 17(5-6), 207-227. doi:10.1080/19393550802492487,2008

[38] S. L. Pfleeger, & D. D. Caputo. Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31, 597 - 611. doi:doi:10.1016/j.cose.2011.12.010, 2011

[39] PriceWaterHouse. Raising security awareness in your employees: The human factor in information security. PWC,2013. Retrieved from http://www.pwc.ch/user_content/editor/files/publ_adv/pwc_raising_security_awareness_e.pdf

[40] C. Russell. Security awareness-implementing an effective strategy. SANS, 2002. Retrieved January 2014, from https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418

[41] L. Navarro. Train employees - your best defense - for security awareness. SC magazine,2007. Retrieved February 23, 2014, from http://www.scmagazine.com/train-employees--your-best-defense--for-security-awareness/article/34589/ , http://www.nsi.org/pdf/awarness-articles/Train%20Employees-Best%20Defense.pdf

[42] M. Johnstone. Security awareness training and privacy. SANS, 2001.

[43] C. L. Anderson & R. Agarwal. Practising safe computing: a multimedia empirical examination of Home computer user security behavioral intentions. MIS Quarterly, 34(3), 613-643, 2010.

Fungai Bhunu Shava
MSc Computer Science (2005), University of Zimbabwe, Harare, Zimbabwe.

BSc Computer Science and Mathematics (University of Zimbabwe, Harare, Zimbabwe.

Lecturer, Department of Computer Science, School of Computing and Informatics, Polytechnic of Namibia transforming into Namibia University of Science and Technology, a PhD student with Nelson Mandela Metropolitan University in South Africa. She has interests in Information security, user-experience, user behaviour and HCI, in underserviced communities. This is her third paper for publication; she has presented her MSc research in 2004 and a poster at SAICSIT in 2012.

Attlee M. Gamundani
MSc Computer Science (2011), University of Zimbabwe, Harare, Zimbabwe.

BSc Hons Information Systems (2006), Midlands State University, Gweru, Zimbabwe

Lecturer, Department of Computer Science, School of Computing and Informatics, Polytechnic of Namibia transforming into Namibia University of Science and Technology.
Doing his PhD in Computer Science in the area of Internet of Things security. Have done many publications in applications use, security and future technologies.