The 5th International Conference on Education and Information Management (ICEIM-2014), Durban, South Africa, June 21-22, 2014

SECURITY E-COMPETENCIES: THE SPHERES AND LEVELS IN THE HIGHER EDUCATION ENVIRONMENT OF SOUTH AFRICA

Author: Mukenge Simon – Tshinu
Cape Peninsula University of Technology (CPUT)
Tel: +27 (0)21 460 3956
E-mail: Tshinus@cput.ac.za

Co-author: Zoran Mitrovic
University of Western Cape (UWC)
E-mail: zmitrovic@uwc.ac.za

Co-author: Michael Twum-Darko
Cape Peninsula University of Technology
Tel: +27 (0)21 460 3291
E-mail: MichaelDarko@cput.ac.za

Mailing address
Mukenge Simon - Tshinu
Room 3.35
Commerce Building
Cape Peninsula University of Technology
Keizersgracht and Tennant Street
Zonnebloem, 8001
Cape Town

The 5th International Conference on Education and Information Management (ICEIM-2014), Durban, South Africa, June 21-22, 2014

SECURITY E-COMPETENCIES: THE SPHERES AND LEVELS IN THE HIGHER EDUCATION ENVIRONMENT OF SOUTH AFRICA

ABSTRACT

This paper attempts to create a conceptual framework for the fostering of security e-competencies in higher education institutions (HEIs). It used qualitative research method where content analysis and induction were used as its data collection and analysis techniques respectively. The rationale for this research is that the HEI is considered as an intensive knowledge creation environment in which stakeholders rely on ICT resources and the Internet to collect, process, store, and distribute this knowledge. As this knowledge and the assets carrying it are shared, the threats from authorised and unauthorised end-users increase. Therefore, given the complexity of the ICT resources in HEI environment, the protection of these ICT resources requires the development of security e-competencies among end-users to be integrated with security solutions. However, these security e-competencies are ambiguously mentioned in the relevant literature, leaving gaps for new research to determine the spheres and levels of skills that end-users need to protect ICT resources in their environment as different jobs in HEI levels require different levels of competencies. The implication of this research is a conceptual framework for the determination of security e-competencies taking into account, the key spheres of ICT security and the needs of different end-users in HEI.

Keywords

Security, e-competencies, ICT resources, end-users, higher education institution

1. INTRODUCTION

The fact that complexity and pervasiveness of the ICT resources allows perpetration against ICT resources from anywhere in the world, using various channels and from various sources (Eminağaoğlu et al. 2009), indicates the current knowledge economy, which is driven by reliance of ICT resources for collection, processing, storage, and distribution of information, requires complex, perverse, and well defined security controls to arrive at acceptable level of securing the ICT resources owned by any organisation. Therefore, this kind of security issues calls for pragmatic security measures that are associate with policies and frameworks (Sattarova, 2013) and that also integrate the physical and human competencies as the emergence of the multi-user systems require the mechanisms to protect the system from its authorised users (and also non-authorised users) and the system's users from each other (Gollmann, 2011:2). During the 1980s and 1990s, the security of the information resources (mostly manual) was made possible by physical security such as locks, bars, and safes. An attacker would only have to travel to the organisation to commit an attack (Jones, 2009). Today, while still recognising the importance and utilising the old protection measures, the interconnectedness, the increased trend of end-users self-developed applications, the power to maintain their departmental websites, and the sharing of information require increased protection of these assets against the complex forms of threats they face. As this information is shared and the ICT resources that carry it are used, the "risk from the authorised (and also unauthorised) users increase" (Williams, 2007) and because of these risks, the ICT resources (including information) need to be protected.

The reviewed literature reports that the end-users who are supposed to be the first line of defense are not properly equipped with the necessary security e-competencies to handle security threats as much of security measures are still technological focused (McCue, 2008). As such, the ICT resources are faced with risks from both trusted and untrusted users. In line with this research, Rainer & Cegielski (2013:85) and Sarkar (2010) precise that human errors or mistakes by employees pose a large problem as the result of laziness, carelessness, or a lack of awareness concerning information security which comes from poor education and training efforts by the organisation. Thus, if the end-users do not keep secret the password, if they cannot protect themselves against the social engineering manipulations, if they cannot change their internet surfing habits, if they cannot update the password or set up the firewall correctly, the ICT resources they access will be negatively impacted.

Competency of end-users, which is part of this study is defined by Eraut (1998) as cited in Guasch et al. (2010) and Chang et al. (2012) as a system of complex actions including the knowledge, abilities, and attitudes required for a successfully completion of tasks. Draganidis & Mentzas (2006) say that "competency is a combination of knowledge (tacit and explicit), behaviour, and skills that gives someone the potential for effectiveness in task performance." Rodriguez et al. (2002) as quoted in Yoon (2009) say it "is a measurable pattern or knowledge, skill, abilities, behaviours, and other characteristics that an individual needs to perform work roles or occupational functions successfully.

In this study, the term e-competencies is used as a combination of knowledge, skills, and abilities (referring also to behaviours) necessary to protect ICT resources accessed by end-users in Higher Education (HE) environments and all these three components are important and interdepend in the development of ICT security e-competencies. Equipped with the information on competency in general, the ICT security defined-competency is defined in this study as "*the application of knowledge, skills, and ability (personality traits) in the ICT environment by to protect ICT resources against unauthorised access and usage with intention of preserving the ICT resources integrity."*

Given their nature and how they can also affect the organisation's productivity, profitability, and confidentiality (Van Niekerk & Von Solms, 2010 and Hayden, 2010:17), the threats and security of ICT resources has become a subject of headline in many organisations, business reviews, conferences (Cavalli et al. 2012). Hence, special laboratories have been set up to investigate the ICT resources security breaches cases. With this reflection in mind, it can be said that gone are the days when the access to computers and other ICT resources was reserved to ICT experts, and gone are the days when the security of ICT resources was reserved to the ICT experts and their specialised security technologies. This study reviewed the literature on ICT resources security with intention to identify the main spheres (themes) of ICT security about which the security e-competencies of end-users be developed to ensure their readiness in protecting the ICT resources they access.

2. THEORETICAL FRAMEWORK

2.1 Current work

From military operations to educational institutions, ICT resources security has received attention and investment in this networked economy that has never been given before (Gollmann, 2011:2). The threat posed by the phishing e-mails received by HEIs, the increased development of computer viruses and key logger applications and other various online and offline threats to ICT resources affect all kind of organisations day and night. Therefore, organisations of any type and size (including HEIs) are required to seek additional security measures in the protection of ICT resources apart from the technological emphasises. In the case of this research, the development of end-users security e-competencies as their access to ICT resources has both positive and negative impact. McCue (2008) demonstrated that *"70% of fraud is perpetrated by insiders rather than by external criminals"*. To worsen the situation in their responses, the author indicates also that organisations focus their controls and monitoring efforts defending the external threats at 90% than on insider threats with technological controls (Vroom, R & Solms, 2004 and Colwill, 2009).

The effectiveness of ICT resources security in the HEI environment as it is in any other business environment needs to be considered from the holistic perspective and multi-level approach. In line with this perspective, Shariati et al. (2011) identified the approaches to information security, which the author classified in four categories, which include (i) security policies and configuration management, (ii) security of enterprise services, (iii) security role management and access control, and (iv) security assessment and requirement engineering. This categorisation includes both the use of security technology and non-technology approach which is the approach suggested by many authors as appropriate for current complex era of security threats affecting the availability and integrity of ICT resources.

In their study on the principles on the areas of employees' compliance with ICT resources security, Siponen & Willison (2009) stressed the need for wide dissemination of security policies to employees, use of software preventives and disciplinary actions for non-compliance and enough full-time security staff. According to Jones (2009), these additional staff will help in addressing the security threats faced by end-users. Siponen & Willison (2009) also cautioned that *"the mere existence of security practice such as policies and education programmes do not guarantee their quality practice."* These practices need to be actively operational and employees made aware of them and updated continuously or empowered with proper security training to be able to be to install security technology (firewalls, antiviruses, intrusion detection systems, etc.) and identify security threats (Smith, 2004).

In another related study, Farn et al. (2008) spoke about the protection of ICT resources "through information assurance (IA) that addresses the full suite of security requirements for today's information infrastructure." This form of integrated information infrastructure security relies on people, the operations, and technology to which policies, procedures, and mechanisms at all layers throughout the organisation need combined to achieve the mission of business and management of infrastructures (Frederick, 2002 as cited by Farn et al. 2008). The same perspective of integrated approach to ICT resources security was also highlighted by Smith (2004) in his study on e-security issues and policy development. Among other components that help in the achievement of more security information resources (ICT resources in general) (i) included security policy, (ii) management support, (iii) budget for security, and (iv) employees. Following the same order of ideas, Okenyi & Owens (2007) proposed the importance of training end-users in the variety of ICT security topics related which need to be grouped in specific categories of ICT security to provide a focused training for security e-competencies development.

The integrated approach to ICT resources security is a way to acknowledge that today's ICT security environment is subjected and influenced by various stakeholders (Hayden, 2010:227), which includes among others (i) the interference by the government at different levels through laws and regulations, (ii) industry associations through best practices, (iii) international bodies through standards, and (iv) customers and business partners through contracts and satisfaction. All these reflect the assumption that merely implementing security technologies, analysis of security log and vulnerability scanner reports are just part of ICT resources security solution and will not be enough for every security case. There is, therefore, a need to have a comprehensive approach in security e-competencies development as the security threats to ICT resources and security measures are broad and dynamic.

2.2 Methodology

This study used a qualitative research method; it relied on previously published materials on ICT security for data collection, and used content analysis for that analysis. The qualitative form of research was found to be a beneficial choice because it can be used well to investigate sensitive and complex topics such as ICT resources security and privacy applied across various entities and has the prospect of discovering rich context related to the study (Zafar, 2013 and Whitman, 2004).

As being the part of a larger project, this part of the study was entirely based on the literature review and the pertinent analysis. In total, seventy-five articles and books were sampled using nonprobability judgmental sampling (Polonsky & Waller, 2011:140-141, 157-158) because the sample must satisfy the requirement for needed content. Forty officially published articles (books included) where analysed for the collection of themes related to the spheres of ICT resources as they enforce or their absence presents a danger for the ICT resources. The rest were not considered because they were either not peer reviewed, not containing the identified spheres, or published before year 2000 then considered outdated. Careful attention was paid in the collection of the themes to avoid their repletion. The MS Excel 2010 was used for collection of the themes and tailing them according to the sphere, and the graph presented in figure 2 was created to show the number of occurrences per sphere.

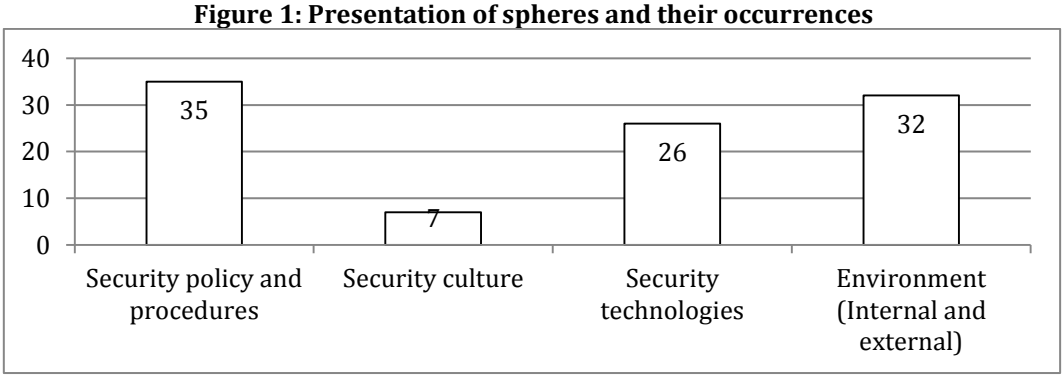
The data were analysed by systematically studying the content (Content analysis) of each published article and document on ICT security to observe and record the frequency of the themes and the way they are presented as they address the spheres of ICT security. The analysis of information of content followed the steps of content analysis described by Welman & Kruger (2001:195-197) which helped in the identification and to relate the phenomenon to the entities, coding, and the occurrence of the themes:

- Firstly, the phenomenon to be studied was clarified, which was the ICT resources security.
- Secondly, the publications in which the content needed to be found, which make the universe for analysis. Only the published articles and books where investigated. Even though the cases could not be referenced as the spheres of ICT security, they should be presented as the means of strengthening the security of ICT resources in particular environment.
- Thirdly, the unit of analysis was coded according to their categories and the occurrences counted in such category. An example of coding was 01 to indicate the first article to number 40 to indicate the last. The categorised themes are those presented in the conceptual framework presented in figure 1: security policy and procedures, security culture, security technologies, and the internal and external environment which include legal aspects.
- Fourthly, the categories were selected according to their nominal levels then were included in the final model.

3. RESULTS AND DISCUSSION

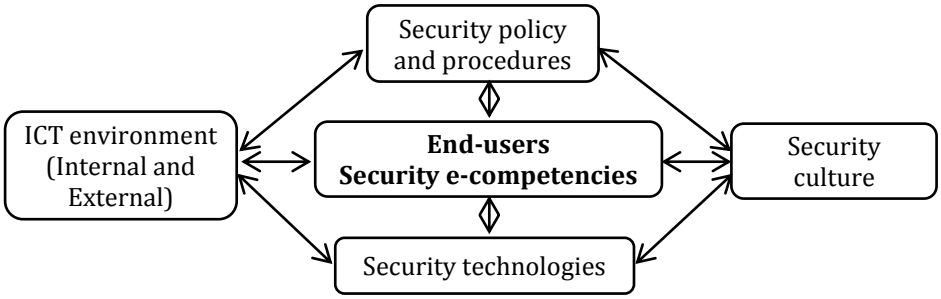
Figure (Figure 1) presents a summary of the findings for this study, which relates to the findings of the study conducted by Fakeh et al. (2012) in which the authors identified four elements (policy, education, knowledge of technology, and behaviour) to be part of security awareness. Because of the limited space gives only a summary of the categories and the occurrence of the themes for the forty units of analysis consulted. The sources of the themes which are acknowledged in the references have been omitted has they could have used forty lines in the graph and prevented the inclusion of the discussion.

Figure 1: Presentation of spheres and their occurrences



From the figure 1 above, the model representing the spheres for security e-competencies can be designed and presented in the following figure (figure 2) and discussed in the following section.

Figure 2: The security e-competencies spheres



This model outlines the fundamental spheres and macro-management of ICT resources risk and security that have a positive and negative impact on the protection of ICT valuable resources about which each end-users needs to develop their security e-competencies and about which other related initiatives such as security policy, culture, technologies, and environment need to be related to. The aim of this exercise was to understand the major spheres that are possible sources of risks to which ICT not only security controls will be applied (Hayden, 2010:8). Also about which the security e-competencies of end-users need to be developed. These areas are briefly discussed below:

- **End-users security e-competencies:** these are in the middle of the above framework (Figure 2) because they are the core to the protection of ICT resources as they relate to all end-users, executives, and security technicians each according to his job requirement in relation to the protection of ICT resources.

  The end-users: end-users at all levels of the organisation (including technicians) have an important role to play in relation to the security of ICT resources they access and the understanding of security policy, culture, security technologies, and the environmental factors surrounding the ICT security competencies and ICT resources. According to Albrechtsen (2007), individual factors such as motivation, knowledge, attitude, and behaviour have an influence on how end-users view ICT security in the HEI environment or any other organisation. In opposition to automated machines that can be controlled and their behaviour predicted in the future, end-users behaviour in relation to ICT resources security is unpredictable and inconsistent (Vroom & Solms, 2004). As such, the control of end-users role in the security of ICT resources becomes difficult and even costly to control even with the installation of security monitoring controls (Vroom & Solms, 2004) will not suffice to fully protect the ICT resources. The approach to ICT resources security in the HE environment should follow the principle suggested by Jirasek (2012) quoted the saying of John Boyd in which he said "It is all about people, process, and technology." But people are the biggest concern among the tree components and are also the most vulnerable among the three (Hall, 2005 as cited in Okenyi & Owens, 2007) as the security infrastructures are made up by people and security technologies are the tools used by people (Hayden, 2010:272-273) in the protection of ICT resources.

  With reference to this study, the development of security e-competencies (necessary knowledge, skills, and behaviour) enforce the security of spheres of ICT resources because the action based on these competences can be used to control these ICT security spheres with due care whenever users access them. As such, knowledge of threats and security measures will need to be described according to the level of employment as to what employees needs to know to protect the ICT resources (Beisse, 2013:35). Skills for a given position in an organisation refer to the capacity to perform a task for a specific job (Beisse, 2013:35), such as the updating of an antivirus. Abilities form the personality traits that influence employees' behaviour and performance (Spencer and Spencer, 1993 quoted in Chang et al. 2012). The traits (behaviour), such as the danger of opening unsolicited e-mails or leaving the desktop account open when leaving the office, will need to be taught to end-users when developing security e-competencies.

  It is important to be reminded that the applied knowledge, skills, and ability need to be measured against previously set criteria or standard and learned in the organizational context (Succar et al. 2013). This is where the difference to ambiguously mentioned training for security lies. The combination of the three elements of security e-competencies and the four levels of competencies

(awareness, supervised practitioner, practitioner, and expert) presented by Holt & Perry (2011:120-122) in the International Council on Systems Engineering (INCOSE) competencies is summarised and the spheres of security e-competencies needed to protect ICT resources in the HE environment will be presented in the following table (table 1) which suggest that for each level and sphere, there should be appropriate Knowledge, Skills, and Abilities (KSA) for that level of employment.

Table 1: ICT security e-competencies development spheres and levels

Spheres / Levels	Security policy and procedures	Security culture	Security technologies	Environment
L4 = Expert	KSA	KSA	KSA	KSA
L3 = Practitioner	KSA	KSA	KSA	KSA
L2 = Supervised	KSA	KSA	KSA	KSA
L1 = Awareness	KSA	KSA	KSA	KSA

- **Security policy:** security policy, according to Jirasek (2012), is a high level document that state both business and security objectives. It is "*technology neutral, concerns risks, set direction and procedures, defines counter measures and penalties in case of transgressions*" (Rees et al., 2003 as cited in Marzieh, 2011). Jirasek (2012), based on Smith (2004) confirms also that the security policy should be approved by the board and sets the accountabilities for ensuring that security objectives are met. As such, security policy should be in the centre of any security related activity that is internal or external to the operations of the organisation. Security policy should also support the elements of personnel security described in the early study of ICT resources security such as screening, security clearances, supervision, and training and awareness (Ettinger, 1993:22), including when selecting security technologies and developing the security e-competencies among the end-users.

- **Security Culture:** an organisation's culture is unwritten but can be observed in its stories, slogans, ceremonies, dress, and office layout (Daft et al. 2010:20). As such, the culture portrays to the external world what the organisation is and believes in concerning particular point of interest. In relation to ICT resources security, it needs to be considered as it drives the attitude and actions of end-users and the adoption of security technologies (Thomson & von Solms, 2006) and the drafting of security policy. Thomson & Solms (2006) believes that organisational culture is one of the drivers of the organisation and affects the employees behaviour to a large extends. As such, it is also a driving force in the achievement of security for ICT resources. It is even important to consider the organisational culture when implementing the security controls and policies.

- **Security technologies:** the innovations in ICT field and reliance on ICT resources for most business transactions, threats to ICT resources are becoming frequent, faster, and dangerous requiring organisations to be ahead in technological expertise to be protected (Sarkar, 2010). These technologies will include antivirus scanners, firewalls, biometrics, and other that will control both inside and outside-driven security attacks.

- **The internal environment:** the internal environment of the HEI on security e-competencies will include culture, structure and authority, security audit, educational programmes, management support, security budget, procedures, and procedures established in the organisation and management of ICT security. These components of internal environment are influential to the employees' beliefs and attitude (Thomson et al. 2006) toward the security of ICT resources as they guide or support their daily actions. Therefore, when developing end-users security e-competencies, they should be knowledgeable about the components within their surrounding and how they affect or contribute to the protection of ICT resources effort.

  An element of internal environment such as the management support and buy-in goes beyond a mere approval of training, such as approval of training and development budget for end-users, proper reporting structure, and serving as a model for security initiative has a positive influence in the rollout and success of security initiative (Hayden, 2010:274,341-345).

  External environment: the interconnectedness of ICT resources across the globe, the collection, processing, and distribution of data and information such as medical records, personal details, and financial information internally and externally, but also externally to business partners has been

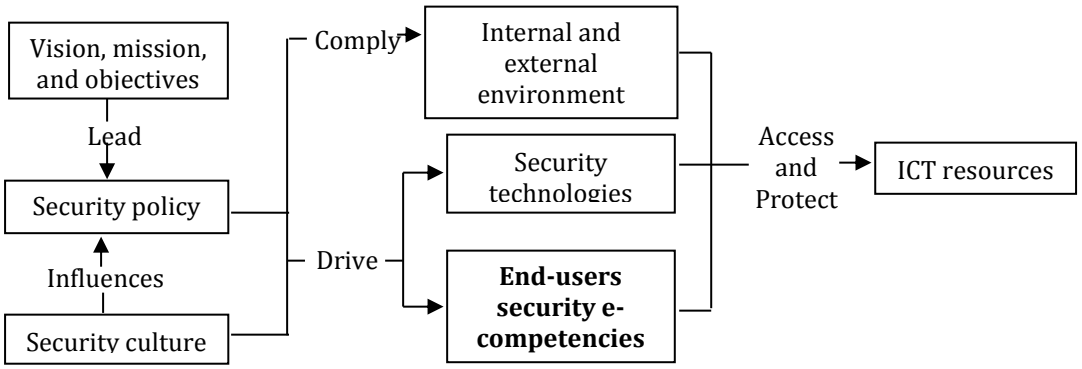
accompanied by various malpractices and negligence (Cavalli et al. 2004). This has prompted governments across the globe to introduce Acts that can regulate the treatment of ICT resources in the organisation. In South Africa, legislations such as the Promotion of Access to Information Act, 2000 and the Protection of Personal Information Act, 2013 have been enacted to regulate the collection, protection, access, and distribution of information by public and private organisations, including the HEIs. This aligns itself to the idea presented by Hayden (2010:272) that maintained that "the security ICT resources begun to be defined in terms of national security" as the knowledge of the one influences the knowledge of the other. Concerning the internal and external environment with relation to HEI security project, it is important to understand this environment is highly politicised, regulated, and has a variety of funding and politics that need to be considered when undertaking security projects (Hayden, 2010:343). This is because of good or bad reason any one among these stakeholders can bring the project at halt. Hence, buy-in from all the key stakeholders in an important step toward the right direction.

The above spheres of ICT security are important even during the risk assessment and vulnerability related to the implementation of comprehensive ICT security measures as opposed to piecemeal security practices that are implemented as a result of the occurrence of security threat by ignoring the overall environment and components directly related to security of ICT resources and source of the attacks. As such, management in the HEI can no longer view the security technologies as the only focus for securing ICT resources, the focus should be shifted to the internal and external environment and issues that have direct and indirect influence on the ICT resources security and the development of security e-competencies. This is because the threats to ICT resources have both internal and external origin. In higher education, there are trends that have forced the development of security e-competencies among the end-users on the spheres identified above.

Among the trends include the reliance on the ICT resources for teaching and learning, the distributed nature of ICT resources across different campus and business partners. For the purpose of this study, if the availability of ICT resources is disturbed due to internal errors or external attacks (such as disruption of network services), there will not be access to online resources, some assignments or exams dates be rescheduled, there will be disruption in the library services, and to some extended access to computer laboratories and other teaching resources will be restricted and classes cancelled. Therefore, the security of ICT resources needs to be maintained at all cost and through the integration of different spheres and by developing security e-competencies among end-users who are in forefront when it comes to the issues related to the security of ICT resources.

Following the determination of the spheres of ICT resources security e-competencies and their levels, it is important to present a value proposition framework for this research in the following figure 2 which also present the importance of this study.

Figure 3: The value proposition for the spheres of ICT security



According to this Figure 3, the development of security policy, which is at the heart of every ICT security activity of any organisation is led by the vision, mission, and objectives of the entity, it is also influenced by the security culture. The security policy has to comply with the internal and external environment of the organisation (which includes the legal environment and best practices) and drives the selection of

security technologies and the development of security e-competencies among end-users which are used to protect the ICT resources which are accessed by end-users to perform their operations.

From the literature reviewed for this publication, various researches containing useful information on ICT security and training. However, each suggesting its own focuses when training end-users on ICT security is presented. Some focus on technological tools and other focusing on non-technological tools, while others combine the two aspects. Even to those that have addressed both technological and non-technological solutions there is a lack of the competencies levels at which these solutions should be addressed when developing end-users e-competencies. This divergence and luck of focus created a gap that this research has tried to close by highlighting the main spheres and competencies levels of ICT security that need to be the focus of ICT training for end-users security e-competencies development.

4. CONCLUSION

The comprehensive literature and its analysis revealed that there is a dire need for protecting valuable ICT resources in today's ICT connected world. The HEIs are not an exception; hence, there is urgent need to make its end-users security competent, i.e. the HEI ICT end-users should possess relevant security e-competences. However, unless the spheres of security e-competencies and related levels of development - combined with knowledge, skills, and abilities (behaviour) be applied to each level of employment that has been identified (and made the focus of each employee's security e-competencies development), the development of e-competencies will be inconsistent and wasted opportunity. Consequently, each employee at particular job will require different set security e-competencies necessary to protect the ICT resources accessed in that environment and through the network.

In the context of this study, it is important to emphasise once again that, the security of ICT resources owned by HEIs is dependent on the security e-competencies of its end-users. This is from the "lower level" end-users to the security technicians and "high level" end-users who use the information stored and distributed through the ICT resources for decision-making, including those executives who make security decisions related to the protection of ICT resources.

REFENCES

Cavalli, E. Mattasoglio, A. Pinciroli, F. & Spaggiari, P. (2004). Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics*, 73(3), 297-303.

Chang, S.H., Chen, D.F. & Wu, T.C. (2012). Developing a competency model for safety professionals: Correlations between competency and safety functions. *Journal of Safety Research,* 43(5), 339-350.

Colwill, C. (2009). Human factors in information security: the insider threat – who can you trust these days?. *Information Security Technical Report*, 14(4), 186-196.

Cooper, D.R. & Schindler, P.S. (2006). Business research methods (9th ed), Singapore: McGraw-Hill.

Daft, R.L., Murphy, J. & Willmott, H. (2012). *Organisation theory and design*. Singapore: Cengage.

Eminağaoğlu, M. Uçar, E. & Eren, Ş. (2009). The positive outcomes of information security awaness training in companies – A case study. *Information security technical report*, 14(4), 223-229.

Ettinger, J.E. (ed.) (1993). Information security: An integrated approach. U.K: Champman & Hall.

Fakeh, S.K.W., Zulhemay, M.N., Shahibi, M.S., Ali, J. & Zaini, M.K. (2012). Information security awareness amongst academic librarians. *Journal of Applied Sciences Research*, 8(3), 1723-1735.

Farn, K.J., Lin, S.K., & Lo, C.C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interfaces*, 30(1), 1–7.

Gollmann, D. (2011). Computer security (3rd ed). United Kingdom: John Wiley.

Hayden, L. (2010). IT security metrics: A practical framework for measuring security & protecting data. U.S.A: McGraw-Hill.

Holt, J. & Perry, S.A. (2011). A pragmatic guide to competency: Tools, frameworks and assessment. U.K: British Computer Society (BCS).

Sattarova, N.I. (2013). Information security of the knowledge economy students. *Middle-East Journal of Scientific Research*, 18(8), 1199-1203.

Jirasek, V. (2012). Practical application of information security models. *Information security technical report*, 17(1), 1-8.

Jones, A. (2009). How do you make information security user friendly? *Information security technical report*, 14(4), 213-216.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, 22(8), 685-692.

McCue, A. (2008). Beware the insider security threat. CIO Jury Insight (2008).

Okenyi, P.O. & Owens, T.J. (2007). On the anatomy of human hacking. *Information Systems Security*, 16(6), 302-314.

Polonsky, M.J. & Waller, D.S. (2011). Designing and Managing a research project: A business student's guide (2nd ed), U.S.A: SAGE publications.

Rainer Jr, R.K. & Cegielski, C.G. (2013). Introduction to information systems: international student version (4th ed), Singapore: John Wiley.

Sarkar, K.R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information security technical report*, 15(3), 112-133.

Shariati, M., Bahmani, F. & Shams, F. (2011). Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science*, 3, 537-543.

Siponen, M. & Willisson R. (2009). Information security management standards: problems and solutions. *Information & Management*, 46(5), 267-270.

Smit, P.J., Cronje, G.J., Brevis, T. & Vrba, M.J. (2011). Management principles: A contemporary edition for Africa (5th Ed), Juta: Cape Town.

Smith, A.D. (2004). E-security issues and policy development in an international-sharing and networked environment. *New Information Perspectives*, 56(5), 272-285.

Thomson, K.L. & von Solms, R. (2006). Towards an information security competence maturity model. *Computer fraud & security*, (5), 11-15.

Thomson, K.L., von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. *Computer fraud & security*, (10), 7-11.

Vroom, C. & von Solms, R. (2004). Towards information security behavioural compliance. *Computer & Security*, 23(3), 191-198.

Welman, J.C. & kruger, S.J. (2001). Research Methodology. (2nd ed), Cape Town: Oxford University Press.

Whitman, M.E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1), 43-57.

Williams, P.A.H. (2007). Medical data security: are you informed or afraid? *International Journal of Information and Computer Security*, 1(4), 414-429.

Zafar, H. (2013). Human resource information systems: Information security concerns for organisations. *Human Resource Management Review*, 23(1), 105-113.