E-ISSN: 2612-4793
Print-ISSN: 2612-4815

Journal of International Cooperation and Development
www.richtmann.org/journal

Vol 5 No 3
November 2022

RICHTMANN PUBLISHING

Research Article

Received: 8 September 2022 / Accepted: 29 October 2022 / Published: 5 November 2022

User Perceptions of Information Security: Evidence from Takoradi Technical University

Olivia Agyemang[1]

Ronald Osei Mensah[2]

Emmanuel Asare[3]

[1]Senior Assistant Registrar, Takoradi Technical University, P.O. Box 256, Takoradi, Western Region, Ghana
[2]Centre for Languages and Liberal Studies, Social Development Section, Takoradi Technical University, P.O. Box 256, Takoradi, Western Region, Ghana
[3]Internal Audit Directorate, Takoradi Technical University, P.O. Box 256, Takoradi, Western Region, Ghana

DOI: https://doi.org/10.36941/jicd-2022-0011

Abstract

This study related to the importance of information and information technology in today's global business. The global nature of information systems also exposes them to threats which make them prone to security breaches. Information risks are several internal and external, making it almost impossible for only information security professionals to handle. This therefore reinforces the need to involve end-users in by educating them to be aware of threats, and their role in curbing those threats. Related information security literature was reviewed to establish the business problem theoretically. Using focus group discussions and open-ended interview guide, data was collected from non-security employees from Takoradi Polytechnic. The data provided understanding of the employees' present security needs, employees perception of information security, employees' personal security initiative, and level of information security awareness. The key findings in the study suggested that, currently some arrangements have been made to ensure information security; however, there is the need for more non-computer-based arrangements such as physical security, training and data backup systems. Further, because some respondents did not perceive the current security arrangement to be adequate, they took personal initiatives like using passwords, using formal communication channels for obtaining information which falls outside their domain or function, and seldom reporting any perceived security threats. These personal initiatives seemed to be the basis for the employees' self-rating of their level of information security awareness, not some training they had acquired.

Keywords: *Educational sector, Information security, Information systems, Security needs, Security awareness, Security management, User perceptions*

1. Introduction

The significance and importance of information has gained a worldwide acceptance in current global business environment. Information systems are now truly pervasive throughout every enterprise across the world. The fast-growing dependence of (if not all) most organizations on their information systems, coupled with the risks, benefits and opportunities Information Technology (IT) carries with it, have made IT governance an increasingly critical facet of overall corporate governance (Williams, 2001). In addition to the factors that benefit business operations such as processing and access to information to a large extent also increase the exposure to risk of computer intrusion, fraud and disruption (Mow, 2012), hence the need for information security which now is considered as inevitable part of IT governance.

Recently, reports shows that information security is gradually improving. However, such improvements may be challenged by the ever-increasing changes to the Internet, changes that raise concerns for professionals as illustrated by a recent survey (CSI,2011). In the same survey, professionals called for improved tools to enhance visibility into networks and web applications most. It is worth noting that these networks and applications increasingly going mobile are used by people (both professionals and non-professionals alike). Hence, information security cannot be left in the domain of security professionals only. There must be efforts to educate and make non-professional system users aware of their roles and responsibilities in ensuring the protection of organizational information assets. This is even more important when the introduction of the Internet into the organization has the tendency to expose internal processes to both internal and external attacks.

While many firms have been seen to operate ineffective information security systems, the porosity within such system could be attributed to the reactive nature used for planning them (Straub and Welke, 1998). The reactive planning nature means that planning is based on incidents that happen around the organization causing the possibility for organizational members to lose touch with managing information security. Efforts made towards studying and knowing about how to avoid such pitfalls especially from the human end of information systems, could increase the level of security within an organization; a key condition to ensuring the availability, confidentiality and integrity of information assets.

2. Statement of Problem

Humans and human behaviours have been discovered as the primary sources of security breaches in organizations (Lacey, 2010; Thomson and van Niekerk, 2012). This aspect could be contributory factors in making perfect security elusive (Bodin et.al, 2008), and so reflect the importance of paying attention to the human element of information security. However, in studying this element, research has been skewed towards the

managerial aspects of information security (Stahl et. al, 2008 as cited in Harnesk and Lindstorm, 2011). Moreover, the awareness dimension of information security (Infosec) as identified in a synthesis of literature posits that more companies and businesses are now focusing on this dimension possibly because of realization that if huge sums of money is spent on technology without a matched level of Infosec awareness, the technology alone would not be enough to ensure security (von Solms, 2001). Despite the practitioner awareness, academic studies have not matched up with studies concerning user awareness of Infosec issues, hence the need for such studies. Undertaking such studies would contribute to a holistic understanding and fill a gap seemingly existing in some studies.

3. Research Objectives

1. To explore the security needs of educational sector employees
2. To examine how current security arrangements meet the employees` needs
3. To explore the employees` personal initiatives to ensure security.

The following core research questions guided the research;

1. What are the security needs of educational sector employees?
2. How does the current security arrangements meet the employees` needs?
3. What are the employees` personal initiatives to ensure security?

4. Significance of the Research

The study is significant in two areas namely research and practice. For research, this study fills the need for user perspective in the information security governance framework for understanding user involvement in planning and implementing a successful information security program. Moreover, it is possibly a cutting-edge study, considering that literature about information security governance in Sub-Saharan African country context like Ghana seems to be arguably non-existent.

This results again should be of interest to practitioners. In practice (for instance during security training), the power and capability of technical protection mechanisms should not be exaggerated. Rather, emphasis should be on its limitations and drawbacks, so that end-users will adopt more cautious security practices and adhere to the requirements of the University's security policies.

5. Literature Review

5.1 Framing Information Security

Computer and network technologies have become very regular features of almost all or all aspects of human life. They are seen in the offices, schools, malls, supermarkets, etc.

However, computer is used to generate so much information, hence the need to prevent unauthorized persons from having access to and using such information-information security (Infosec). Information security has become even more important considering the increasing usage of the Internet which is largely seen as insecure due to its very wide range of geographical spread. Information security could be described as a state of being free from unauthorized use of the system and its resources; misuse of the system and its resources; and disturbance of the system`s operations. The concept of Information security can also be defined as a service for ensuring prevention and control (Enescu, Enescu, and Sperdea, 2011), typically of an organization`s information and electronic resources. It is apparent that either definition is more vivid as seen within aspects of information security (Infosec).

The following aspects embodies what is expected of information security (Infosec). They include confidentiality, integrity and availability of an organization`s valuable information (Miller, Harris, Harper, VanDyke and Blask, 2011). Other aspects advocated in the literature include non-repudiation (Shirtzand Elovici, 2011) and authenticity (Feruza and Kim, 2007). Interestingly, there is partial deviation and agreement in another list of 'seven pillars of security' which include authentication, authorization, privacy, integrity, non-repudiation, availability and audit (Kapoor, Pandya, Sherif, 2011). These viewpoints are collated and presented in the table below.

Table 1. Various aspects of information security

Publication	Information security aspects
Pfleeger and Pfleeger (2007) Miller et al (2011)	Confidentiality, Integrity and Availability
Shirtz and Elovici (2011)	Confidentiality, Integrity, Availability and Non-repudiation
Kapoor et al (2011)	Authentication, Authorization, Privacy, Integrity, Non-repudiation, Availability and Audit
Feruza and Kim (2007)	Confidentiality, Integrity, Availability, Authenticity, No-repudiation
(Ma, Johnston, and Pearson, 2008)	(information) Integrity, Confidentiality, Accountability, Availability

Authentication as prescribed by Kapoor et al (2011) is towards consistently informing various users apart that, anyone who intends to access a computer system or some information is really allowed to do so. Usually, passwords provide a defense mechanism to control who accesses computer and information resources possibly because it is relatively inexpensive and easy to deploy and manage (Yang and Choi, 2010). Hence, one could argue that confidentiality as prescribed by Miller et al. (2011), and Shirtz and Elovici (2011) could be ensured if users are expected to 'identify' themselves. Consequently, people who do not have the right usernames and or passwords can neither login to the computer nor have access to the information therein.

5.2 Information Security Research: Issues and Evidence

This section adopts aspects of the Information Security Governance framework by Da Veiga and Ellof (2007) to discuss research from 2007 until 2012. The framework is useful because;

1. It can be used by an organization to govern information security by creating guidelines and controls to address risks.
2. It can be used to manage employee information security behaviour.
3. It provides a means to implement a holistic information security program covering technical, procedural, and human components.

There are four levels (A, B, C and D) within the framework. Level A components include strategic, managerial and operational, and technical. Each of these level A components have their respective level B correspondents. For example, Strategic component has leadership and Governance, Managerial and Operational has Security Management and Organization, Security Program Management, and user Security Management, whilst Technical has Technology Protection and Operations. Leadership and Governance refer to executive level sponsorship for information security, as well as commitment from management and the board to protect information assets. The above characterization has been illustrated in the table below.

Table 2. Components of Information Security Governance

Level A Components	Level B Components	Level C Components
Strategic	Leadership and Governance	Sponsorship
		Strategy
		IT Governance
		Risk Assessment
		ROI/Metrics/Measurement
Managerial and Operational	Security Management and Organization	Program Organization Legal and Regulatory
	Security Polices	Policies
		Procedures
		Guidelines Certifications
		Best Practice
	Security Program Management	Monitoring and Audit
		Compliance
	User Security Management	User Awareness
		Education and Training
		Ethical Conduct
		Trust
		Privacy
Technical	Technical Protection and Operations	Asset Management
		System Development
		Incident Management
		Technical Operations
		Physical and environmental
		Business Continuity

5.3 Security Management and Organization

This aspect within the Information Security Governance framework covers Program Organization, and Legal and Regulatory considerations of information security. The former covers information security organizational design, composition and reporting structures, roles and responsibilities, skills and experience, and resource levels in the enterprise security architecture, whilst the latter covers the various national and international legislations needed to be considered to ensure information security.

Even though security programs and controls are important, there is some variance in how security is interpreted. This requires "a progressive shift in emphasis from processes and procedures towards people, relationships and information flows" (Lacey, 2010, p.12). The people within the organization, consequently have a role to play in ensuring security. Nevertheless, roles and responsibilities cannot be assigned without the knowledge of the people to execute them. Hence, the need for awareness using tools like the information security vocabulary test to assess awareness levels, and to guide the content of awareness programs (Kruger, Drevin, and Steyn, 2010).

Apparently, such programs that test people`s awareness levels could be followed by implementation of actual programs to increase awareness and continuous evaluation to assess the program`s effectiveness. According to Abbas, Magnusson, Yngstrom, and Hemani (2011) evaluation forms the subject of study. They noted that security evaluation processes could be quite lengthy and time-consuming, and risk being obsolete because new threats are constantly emerging.

This observation suggests the need for continuous and dynamic monitoring, awareness and evaluation program that keeps the organization and its members security-conscious.

Similarly, whilst the organization makes internal efforts to ensure security, there is some expectation to extend such efforts to external environment too. For instance, firms are advised to consider external forces such as national laws (Ma, Johnston, and Pearson, 2008) in the design of their security programs. Moreover, the situation where e-commerce companies do not inform their customers fully about the privacy policies (Desai, and Phelps, 2012) leaves much to be desired. As a stopgap measure, consumers are advised to read the policies and understand what their information would be used for.

5.4 Security Policies

An information security policy is the first requirement for planning, implementing and maintaining an organization`s information security (Pathari and Sonar, 2012). Without a good security management policy (and practice), a technical security solution alone is not enough to protect an organization because it needs people to operate and manage (Chang and Lin, 2007). This argument could still hold even though there may be

emerging systems (SIMs) that seeks to remove or reduce human involvement (Mitropoulos, Patsos, and Douligeris, 2007; Abbas, Magnusson, Yngstrom, and Hemani,20011). A security policy is a result, embodiment of how management expresses a general intention and direction. Policies should however take into consideration the aspects mentioned under Security Management and Organization. Within the ISG framework, the components under this theme include Policies, Procedures, Standards, Guidelines, Certification and Best practice.

According to Garrison and Ncube (2011), security breaches which involved information theft and information exposure are more likely to occur, but could be reduced by decreasing carelessness, increasing training and quality assurance and instituting appropriate policies. In the same, many of these security threats and violations are caused by a failure of the users to comply with the existing security policies of the organization (Enescu, Enescu, and Sperdea, 2011). Hence, the importance of policies cannot be overemphasized. And earlier empirical examination of the importance of policies supports this too. Abu-Musa (2010) studied the existence and implementation of information security governance in Saudi organizations.

The study revealed that although a majority of these organizations accept the importance of ISG for the success of IT and corporate governance, they did not have written information security policy statements. The questions to ask then is, if there is increase number of violations because laid down statement are not being followed, then what happens if they (laid down statement) do not exist at all? Furthermore, if there is no written security policy statement, how much more security awareness policy? Others argue nonetheless about the insufficiency of information security awareness policy in ensuring information security if it is not based on the culture of the intended targets (Chen, Medlin, and Shaw, 2008).

Regardless of which plan exists-security plan or the security awareness plan-there is the need to communicate it through awareness and training. Doing so ensures that information security goals form a part of the organization`s identity (Thomson and van Niekerk, 2012).

Additionally, employees` information security goals should be compared with the information security goals of management so that differences would be identified and evened out. Making all organizational members part of the security plan is paramount because security components are more effective and efficient if the system is intrinsically secure (Enescu, Enescu, and Sperdea, 2011). The extent to which an organization`s information security plans succeed determines how information assets are protected (Kruger, Drevin and Steyn, 2010).

5.5 Security Program Management

This theme in the Information Security Governance captures the need to measure and enforce compliance, and to monitor both technology and employee behaviour to ensure

compliance with information security policies. Studies have explored the use of technology to ensure compliance with laid down policies. For instance, the usability of two image-based authentication methods is assessed in a web-based environment (Jali, Furnell, and Dowland, 2010) it could be seen from the focus of the measures mentioned in that study that, there is some dominance on technical measures and control mechanisms to achieve compliance. Hagen, Albrechtsen, and Hovden (2008) corroborate this argument (as mentioned in the previous section) after the assessment of the implementation of security measures that, even though awareness-creation activities are more effective, they are applied with less seriousness than technical administration measures.

5.6 User Security Management

The importance of managing users (or humans) in the information security effort cannot be overemphasized, due to the evidence supporting the argument that humans are the weakest link, human behaviour is the primary source of security breaches in organizations, rendering technical measures and policy insufficient (Lacey, 2010; Thomson and van Niekerk, 2012). Some of the technical measures include intrusion detection systems (IDS) (Debar and Viinikka, 2006), passwords (Yang and Choi, 2010), biometric-based systems (Ahmed and Siyal, 2005; Jain, Ross, and Pankanti, 2006) cryptography (Feruza and Kim, 2007; Kapoor et al. 2011) amongst others. Even though there is a call for further research into technological or technical solutions to Infosec, the effectiveness of such solutions to a large extent depends on the users` know-how and ability to use them (Chen, Medlin, and Shaw, 2008) and how they match existing social conditions (Crane and Pearson, 2011).

It therefore makes sense that seventy-one (71%) of companies provides security training to employees (Deloitte, 2010). The inclusion of the User Security Management within the ISG to address user awareness, education and training, ethical conduct, trust and privacy is accordingly welcoming. But as has been noted, end-user security has been studied as if it was independent of technical security mechanisms examining factors like personal traits, cost-benefits habits amongst others, and somewhat ignoring the possible impact that end-users' perception of technical security protection could have on their intention to follow security policies (Zhang, Reithel, and Li, 2009).

It is noted that even though there may be varied techniques for managing information security, there is some stress on the need for control and discipline (Harnesk and Lindstrom, 2011). With an underlying aim of improving design of Infosec training and awareness programs, an extension of the issues under user security management has been done to include behaviour. However, studies about this concept have been concerned only about how users comply with security policies (Harnesk and Lindstrom, 2011). This study broadens the understanding of security behaviour with a typology which is based on the dimensions of discipline (security management) and

agility (security in use) to understand the relationship between them. The study argues that security procedures should be intertwined with users` interpretations of the procedures.

Whilst this view is supported (Lacey, 2010), it contrasts with others expecting good security behaviour to result from training and awareness programs (Zhang, Reithel, and Li, 2009). The use of web increases the need to be aware of and act towards achieving and maintaining security. The increasing use of technology in communication, collaboration and interaction introduces new threats like online predators, the theft of user data, and viruses (Futcher, Schroder and von Solms, 2010). Also, web applications store sensitive user information thereby, the introduction of a plug-in to detect, prevent and record web attacks based on an identified pattern (Kapodistria, Mitropoulos, and Douligeris, 2011). The solution introduced was however, for the server side of web applications, hence falling short of addressing issues on the user side of web usage. One such issue relates to educating users about privacy considerations of techniques, making users act based on perception, hence a similar we-based tool to educate users (Wills and Zelijkovic, 2011). They developed a web-based tool that informs users about which third-party sites are tracking information from sites intentionally visited. The study showed that some know about the privacy issues online, yet do not take any actions for reasons which were not explored by this study. Others use anti-spyware when faced with online threats (Gurung, Luo, and Liao, 2009). Negligence and carelessness on the part of user cannot be ruled out as a cause of security threats and a source of increase exposure and stolen incidents (Garrison and Ncube, 2011; Workman, 2008). The ability of aforementioned tools to forestall the threats posed by negligence and carelessness is in doubt. The people related issues that the deficiency of technical measures highlight, mirrors the impossibility of leaving out social issues in information systems discussions. Including people and social issues in the quest for information security is therefore plausible.

In as much as some security threats are caused by human apathy (Thomson and van Niekerk, 2012), human negligence (Garrison and Ncube, 2011), carelessness (Workman, 2008), others are caused deliberately due to reasons including financial hardship relationship strains, substance abuse, and job changes (Shropshire, 2009). It seems that human measures are needed to solve human problems hence the proposal to use vigilance on the part of managers and peers to minimize insider threats (Shropshire, 2009). Another human solution to the observed problem could lie in how security risks are communicated. In addition to calling for more supporting empirical evidence, Pattinson and Anderson (2007) argues that end-users are likely to show desirable information security behaviour if their perceptions of risks associated with threats are increased by manipulating risk communications; by including human factor variables.

Additionally, even though education and training for users seems to be a way out (Sun, Ahluwalia, and Koong, 2011), communicating information security awareness

information is still faced with challenges due to the lack of formal methodologies; informing end users is still quite technocratic; awareness information should have content from the audience themselves (Stewart and Lacey, 2012).

6. Materials and Methods

6.1 Research Design

The type of research and researcher goals usually define the research approach used by the researcher, (Robson, 1993). In exploring ways to answer the research questions posed for this study, the researcher adopted the qualitative approach as the method of study. This approach was chosen because it enables an in-depth inquiry into the research problem. In this regard, the focus group discussion strategy was used in gathering data about Takoradi Technical University, which is the case study organization. Data collection involved three group interviews with different groups of employees. The first group was made up of employees from the University`s Central Administration, Planning Unit, and Public Relations Unit. This group is collectively referred to as 'CPP Department'. The second group comprised of employees from the Academic Section (Examinations Office and Admissions Office), and is collectively known as the 'AS Department'. The third group includes employees from the Finance department, and Internal Audit department. This group is collectively referred to as 'FI Department'.

6.2 Focus Group Discussions as a Research Method

Focus group is "... a carefully planned discussion designed to obtain perceptions on a defined area of interest in a permissive, non-threatening environment" (Kreuger, 1988). It normally involves an individual obtaining information about a pre-determined purpose from an assembled group of between six to twelve people (Prince and Davies, 2001). The aim is to gain detailed knowledge about a topic area. Using this method, a discussion is generated about a specific topic. A facilitator who is in charge of developing the exploration and development of the topic leads the discussion. The discussions about the topic generate in-depth non-quantitative data (Jinks and Daniels, 1999), and not results for use in statistical projections (Leitao and Vergueiro, 2000).

6.3 Population

The number of participants in the focus group discussions ranged between six (6) and seven (7). They were chosen from different units in the University in consonance with the expected diverse nature of focus group participants (Morgan, 1996). The specific distribution is illustrated in the table below. The distribution across departments also ensures "diversity of variations" which contributes to the validity of this study (Hellstrom and Husted, 2004).

Table 3. Distribution of Focus Group Participants according to the Departments

Department	Number of Respondents
Central Administration	4
Planning Unit	1
Public Relations Unit	1
Academic Section Examination	4
Admissions	3
Finance	3
Audit	3
Total:	19

6.4 Sample (Respondents selected) Sampling Procedure

The study needed people who were involved in gathering, processing, generating, managing, storing, using and giving information at the University. Accordingly, the Central Administration (HR, Planning, Records (Staff) and Dispatch, Academic section (Examination Unit, Admissions, Students' Academic Records Unit), Finance, Internal Audit and Public Relations Units were considered for study.

Participants were formally invited to participate in the study after gaining permission from the institution`s Registrar. Those interested were supposed to fill a sheet attached to the letter, and returned to the department`s heads. The department heads then scheduled different dates, times and venues with the facilitator (researcher). The researcher and the signed-up participants were notified of the meeting schedule. The various groups represented a sample of individuals that had something to say about information security- a very important feature in the focus group method as noted by Hellstrom and Husted (2004). The participants` demographical and occupational information are presented in the table below.

Table 4. Demographic and Occupational profile of Focus Group Participants

Occupations	Gender	
	Male	Female
Administrators	10	4
Accountants	2	1
Internal Auditors	2	0

6.5 Data Collection Procedures

Primary data was collected through a semi-structured questionnaire with open-ended questions used for the focus group discission. Initial secondary data about the number of staff in the various departments were obtained from the University`s official website and planning unit. This was necessary in order to plan and organize the various groups of participants. In conducting this study, the instruments of research adopted were

interview guide for interview as well as focus group discussions. Face-to-face interviews with focus group were used because of the high possibility of yielding the needed response, and the tendency of the highest response rates. This method also gives the interviewers room to observe the other forms of nonverbal communication and gestures of respondents whiles responding to the questions posed by the researcher.

One important step in conducting the discussions was to ensure that the participants were comfortable to speak with honesty and openness. Respondents were assured of anonymity; their names were not captured accordingly. Also, participants had prior knowledge of the session through a letter which had been sent to the Registrar`s office, and distributed to all department heads.

Interestingly, some of the participants were not comfortable to have their responses captured on tape and so the Facilitator conspicuously used the recorder`s pause function, when those participants needed to speak. Such respondents were however comfortable with pen-based note taking by the facilitator. Overall, at the end of each session, the facilitator related the information gathered from the discussions back to the groups. The necessary changes were made to inaccurate representations and interpretations of their responses.

6.6 Instruments

This study sought to capture the deeper perception of non-security employees about information security. Consequently, the main instrument used for the study was an open-ended interview guide which had questions posed to the focus group participants. The topics in the interview guide were carefully selected to help expose the deeper meaning of the participants about information security in their workplace.

6.7 Data Analysis Procedure

The analysis started with the transcription of the notes from various sessions with the participants. In addition, the researcher listened to, and transcribed the tape-recorded responses verbatim. The transcripts were read over several times, and organized under the themes guided by the research objectives. This allowed filling in information gags, and using interesting quotations made by some of the participants. Different recording equipment had been tested, and the best one chosen so, there was no problem with sound or quality of recorded material.

7. Presentation of Data and Analysis

7.1 Present Information Security Needs

Respondents were asked what their present security needs were. This question was to

find out the physical tools that employees need to ensure information security. Six (6) staff members in the CPP, seven (7) for AS, and six (6) for FI department said they needed a backup system. Similarly, the same distribution said they needed antivirus software. On the other hand, 4, 7, and 4 for CPP, AS and FI departments respectively said they needed firewalls software.

In addition, whilst five (5) staff members each for all three departments needed physical security, 6, 7 and 6 said they needed training. The data is represented in the table below;

Table 5: Information Security Needs of Non-ICT Staff

Non-ICT Staff				
Department	CPP	AS	FI	Total
Backups	6	7	6	19
Antivirus	6	7	6	19
Firewalls	4	7	4	15
Physical security	5	5	5	15
Training	6	7	6	19

7.2 Employee Perception of Information Security

Do you think there are enough measures in the University to protect your identity?

This question was to find out how the staff members perceived the level of security in the University, and whether the current measures were enough to ensure that their identity was protected. A Yes response indicated that the respondent agreed to the adequacy of measures in response, there were 4 No, 2 Yes from the CPP department; 5 No, 2, Yes, from the AS department; 3 No and 3 Yes from the FI department.

Do you think there are enough measures to protect your information?

This question was to find out staff perception about the adequacy of measures to protect information. Within the CPP department, there were 5 No and 1 Yes; in the AS department 4 No, and 3 Yes; and in the FI department 4 No, and 2 Yes.

Table 6: Employees` Perception about Information Security

Respondent No.	CPP	AS	FI
1	4	7	8
2	7	7	8
3	7	5	8
4	4	3	8
5	3	8	5
6	8	9	7
7	–	8	–
Average Score	5.5	6.7	7.3

7.3 Employees' personal security initiatives

Have you ever done any activity that caused a security problem?

This question was to enquire from employees if they had ever engaged in any security threatening activity. Interestingly, all but one (from the CPP department) had ever engaged in such an activity. Further, none of the respondents in either the AS or the FI department had supposedly engaged in any security-breaching activity. A follow-up question was posed to the single respondent (who had engaged in the security threatening activity)

What kind of institutional information do you work with?

This question sought to understand the type of information the employees handled to inform the level of sensitivity, and hence, the related level of awareness and or alertness required to ensure information security. Employees in the CPP department handle the Vice- Chancellor's correspondence, human resource information including staff records, general administrative documents, University publicity and media information, student records, and other stakeholder information including alumni records. On the other hand, the AS department work with prospective student records, examination results of applicants, students' academic records, records of deferred and rusticated students, students' admission information, course curriculum, examination information, and some information on University's stakeholders.

The FI department handles accounting, auditing, some human resource, financial, employee payroll, and student enrolment and payment records.

Do you lock your PC when absent from it?

This question was to find out how respondents take simple security initiatives like logging off computers that were idle or not in use. From the CPP department, whilst 3 respondents said they did not lock their PC, 3 did lock. Within the AS department, whilst just one (1) did not lock, as many as 6 said they did lock their PCs. Similarly, within the FI department 5 out of 6 respondents said they locked their unattended PCs. One respondent added that;

> *I shut my PC whenever am leaving". Also, another respondent explained that she didn't lock her PC because she "shared it with another user". Another respondent does not lock it because she shared neither the PC not the office with any other person. She added "Locking the door is enough.*

Which of the following methods do you use to remember your password?

This question sought to understand how respondents treated and remembered their passwords. This question was inapplicable to two respondents from the CPP department because they did not have passwords. The other responses are captured in the table below;

Table 7: Methods used by employees to remember their passwords (CPP)

CPP Department Respondent	Methods of Remembering Password
1	**a, b, c, & d**
2	**b, c, e & f**
3	**a, c,** & **e**
4	**a & e**

Within the AS department, all respondents had passwords. The table below shows how the respondents said they remember their passwords.

Table 8: Methods used by employees to remember their passwords (AS)

AS Department Respondent	Methods of Remembering Password
1	**b, c, & e**
2	**b & c**
3	**b, c & e**
4	**a, b, & e**
5	**c & e**
6	**b, c, & e**

Within the FI department just one respondent did not have a password. The responses of the other five (5) are captured in the table below.

Table 9: Methods used by employees to remember their passwords (FI)

FI Department Respondent	Method(s) of Remembering Password
1	**b, c, & e**
2	**b, c, & e**
3	**e**
4	**a, e, & f**
5	**c & e**

Legend for Tables:

a. I never change my password
b. I share my password
c. I choose a simple and easy to remember
d. I ask someone else to help
e. Memorize
f. Write down
g. Store on my phone

7.4 Level of Respondents' Information Security Knowledge

This question sought to understand whether respondents knew what information security threats are. Only one (1) out of six (6) respondents in the CPP department did not know what they were. Within the AS and FI departments, the thirteen (13) respondents said they understood information security threats. Furthermore, they were able to give varied examples of threats to computers and information. Some of the threats mentioned include intrusion, viruses, hackers, flood, fire outbreaks, alteration, shared password, shared PC, spam, and use of storage devices. Very encouragingly, they also know how to secure against these threats.

They also mentioned measures like using anti-virus software, using passwords, and locking information in cabinets.

7.5 Employee Information Security Awareness level

To test the level of employees' information security awareness, researcher asked respondents if they knew of the existence of a plan and/or program to secure information. Within the CPP department, all six (6) respondents said there was no plan, as did all five (5) in the AS department. Interestingly whilst four (respondents) in the FI department said No, two (2) said there was.

To understand why only two people knew of the existence of such a plan, researcher asked those two respondents. Their responses pointed to their involvement in certain committee-level assignments and prior use of some documents as sources of their knowledge of the existence of a security plan. Disturbingly, only one of the two respondents who had knowledge of the plan's existence, had actually looked at the contents of the plan. In a short description of the plan, "*it was not adequate"*.

Within this study, some findings conflict with an earlier one; respondents previously suggested that they had received information security training during which they were informed about where they could report information security incidents. It is unclear the contents of the training, because when asked explicitly whether they had received any training in information security, five (5) out of six (6) respondents in the CPP and FI departments said they had not. Also, all seven (7) of the respondents from the AS department said they had undergone training. The respondents who had training vividly remember that they received training which was organized by MAC Edu Consult when the University was about to implement online system for admission and student registration.

This training may have been directly related to handling the new online admission and student registration application, and not for general information security procedures. This is because when respondents were asked whether they knew either the institution's code of conduct i.e., the rights and wrongs of handling information or security policy, there were varying responses. For instance, whilst none of the twelve

(12) respondents in the CPP and FI departments knew of a code or policy, only one (1) in the AS department knew. In addition, whilst no one in the CPP department had received training on how to handle institutional information, only three (3) and one (1) in the AS and FI departments respectively had received such training. Overall, the table below shows how respondents rated their level information security awareness levels on a scale of 1 to 10 (i.e., 1 for lowest, and 10 for highest).

Table 10: Overall Security Awareness Level

Respondents	Departments		
	CPP	AS	FI
1	6	4	5
2	4	8	8
3	4	8	9
4	6	7	8
5	7	4	4
6	5	8	6
7		7	

8. Analysis and Discussion of Findings

8.1 Present Information Security Needs

Findings from the focus group discussions presented revealed that the non-ICT staff members in Takoradi Technical University have security needs which seem to be currently unmet. These needs could be grouped into computer-based needs and human needs. The computer-based needs include hardware and software. The hardware needs include Uninterruptible Power Supply, and a file backup system. On the part of software, the related needs are antivirus and firewalls. In addition, the main non-computer related needs are training (in information security) and physical security (e.g., locks for sensitive information especially backup devices).

The employees' mention of these needs suggests the low-level or possible absence of these facilities or conditions. The current situation does not promote a high-level of information security practice in the organization. For instance, work files risk a single point of failure when the original storage points cease because there is no (working) backup system. As the respondents rightly mentioned, there was a need for training in information security. This is agreeing with previous study that increasing training is one way to reduce information security threats (Garrison and Ncube, 2011).

Similarly, as mentioned in the literature review, many security threats and violations result from users' failure to comply with existing security policies of the organization (Enescu, Enescu, and Sperdea, 2011). One question that arises is, what if users are not aware of the contents of such policies and/or how what constituted compliance or non-compliance? A response to this question reiterates the need for

training for users so that it would be easier to ensure security. After all, training amongst other awareness-creation measures is more effective (Hagen, Albrechtsen, and Hovden, 2008).

8.2 Employee Perception of Information Security

From the responses, it seems that the level of information security in research setting is quite low. For instance, a greater number of the respondents opined that the current measures to protect their identity was not enough. Even though the study does not go further to ask the specific measures they will like to be in place, it could be deduced from the unavailability of the 'basic' needs in the previous section, that more advanced identity protection measures were not available either. This was a situation that lowered the respondents' perception of experiencing identity protection. In addition, respondents do not think there are enough measures to protect information either.

As already mentioned, if there are 'basic' needs for backup systems and antivirus software, then there is some logic in the perception that the majority of the respondents hold about low protection for information. Other related responses to a question about the level of protection for information assets like computing equipment corroborate this view – that there is low information security. The majority (10 out of 17) of respondents thought that the level of protection for the institution's information assets is low.

Even though passwords are used to ensure the safety of 'soft' information (or information not printed out on paper), little had been done or is done to secure information on printed matter.

This situation lends some credence to the earlier identification of physical security as an information security need. Also, within previously discussed literature, it has been noted that the extent to which an organization's information security plans succeed is somewhat determined by how information assets are protected (Kruger, Drevin, and Steyn, 2010). Hence, if there is low protection of information assets, then it is obvious that respondents' perception of security would be low.

Furthermore, research participants' responses to the question about their concern for information security suggest that employees are willing to cooperate and/or abide by procedures and measures instituted to ensure security. Also, one may draw a link between their supposed concern for information security and the kind of information the respondents handled. Even though this is treated in detail in a subsequent section, drawing a link could help in understanding the eagerness towards information security. For instance, whilst some of the respondents work with high-level (and confidential) correspondence, personnel records and student admission and examination records, it seems there would be a natural tendency to protect such information. In the same vein, it is important to note how respondents felt about their colleagues' concern for information security. In terms of average of a 10-point scale (1 for lowest, and 10 for

highest), those in the Central Planning Unit had the lowest score of 5.5, followed by the Academic section with 6.7, and 7.3 for the Finance and Audit. These perception ratings could be basis for arguing that employees could influence the information security behaviours of their colleagues. We could also infer from the type of information that perhaps due to the monetary information that the third department handled; they had the highest propensity to face security risk. The employees in that department expected each other to be on an alert level that surpasses that of those employees that handle correspondence for instance.

8.3 Employees' personal security initiatives

Previous studies have found that humans and human behaviours are primary sources of security breaches in organizations (Lacey, 2010; Thomson and van Niekerk, 2012). However, this study shows that not all human behaviour is deliberately or non-deliberately exhibited to cause a security breach; some of them are done to prevent breaches. From the responses, it seems the staff members are cautious to the extent that they know and stay away from actions and/or inactions could result in a breach. It may hold true that a shift from focusing on processes and procedures towards people, relationships and information flows (Lacey, 2010, p. 12). Such a change may be in the right direction considering that a majority of the respondents in this study have ever faced the need to obtain and use information which they did not have traditionally. How then is such information obtained? This question relates to information flow, which is a new point of focus for securing information (Lacey, 2010, p. 12). Interestingly, it seems that there are laid down means like letters, memos, and (released) committee reports, for acquiring non-departmental information. The current arrangements therefore suggest that if any information is acquired outside these official information flow channel, it could be regarded as a breach, which may then be traceable.

The response from one of the CPP department's staff about information disclosure could hold some credibility, especially going further to describe how he/she overheard people discussing that information – people who are ordinarily not supposed to ever have access to that information. The question which arises is how such information left its storage point to get into unauthorized persons. Interestingly, this breach was not registered at the place designated to receive, record and act on such incidents – the ICT Services Department. Why was this breach not reported? Did the victim not know where to report it, or did the victim deliberately ignore the disclosure. Did the choice to ignore it have anything to do with the type of information?

These are questions that could be posed not only to that victim, but generally to those other respondents who said they did not report security incidents. Even though they had received some training, and had been told where to report security breaches, some did not report.

In addition, the findings suggest the importance of relationships in the quest for

information security. This is because even though some a majority of respondents used and maintained passwords (at least for their computers) some could not use passwords because their computers were shared. Nonetheless, the methods used by respondents to remember passwords leaves much to be desired. The findings suggest that as many as 9 respondents shared their passwords as a way of remembering them. Also worrying is that respondents choose a simple and easy to remember password, and that just one respondent only memorized his/her password. Encouragingly, only one respondent wrote down his/her password. The current situation suggests that employees have limited education on the use and management of passwords as sensitive information that should be hard to guess, and not disclosed under any circumstances nor for any reason. Overall, these findings also suggest that the effectiveness of security measures like passwords (Yang and Choi, 2010), is somewhat dependent on users' knowledge and ability to use them (Chen, Medlin, and Shaw, 2008). As a consequence, if users do not know how to choose complex passwords, and or how to modify passwords, they would use other means that could result in security breaches. For instance, an authorized person may chance upon a password, which has been written down (by an originally authorized person).

Furthermore, existing social conditions between users could determine the how effective technical measures are (Crane and Pearson, 2011).

Hence, it makes sense that currently some respondents shared their passwords with other people as a way of remembering. This also suggests that information exposure could be reduced by decreasing carelessness, increasing training and quality assurance and instituting appropriate policies (Garrison and Ncube, 2011).

8.4 Level of Respondents' Information Security Knowledge

This question sought to understand whether respondents knew what information security threats are. Only one (1) out of six (6) respondents in the CPP department did not know what they were. Within the AS and FI departments, the thirteen (13) respondents said they understood information security threats. Furthermore, they were able to give varied examples of threats to computers and information. Some of the threats mentioned include intrusion, viruses, hackers, flood, fire outbreaks, alteration, shared password, shared PC, spam, and use of storage devices. Very encouragingly, they also know how to secure against these threats. They also mentioned measures like using firewalls, anti-virus software, using passwords, and locking information in cabinets.

8.5 Employee Information Security Awareness level

The findings presented under this theme suggests that if a security plan really exists, then not all end-users are aware of it, and do not know the part they should or could play in its execution to ensure information security. It may be true that a security

management policy or plan is important (Chang and Lin, 2007). However, there is equal importance in communicating that plan through awareness and training. This main reason for doing this is to ensure that information security goals form a part of the organization's identity (Thomson and van Niekerk, 2012). Users would also know their role, rights and responsibilities, and the consequences of their actions/inactions.

The insight given by the respondent about the supposed inadequacy of the existing security plan suggests that there is a mismatch between what is needed on the ground, and what the plan caters for. However, previous work has stated the need to compare employees' information security goals with the information security goals of management so that differences would be identified and evened out (Enescu, Enescu, and Sperdea, 2011). It is also important to make all organizational members part of the security plan because security components are more effective and efficient if the system is intrinsically secure (Enescu, Enescu, and Sperdea, 2011). Overall, the self-ratings by the respondents about their information security awareness level seem to hinge on self-preparedness and personal effort, and not a holistic organizational program to achieve and maintain information security.

9. Summary of Key Findings

This study relates to the importance of information and information technology in today's global business. The global nature of information systems also carries with it some threats to how secure information is. Information is exposed to risks both internally and externally making it almost impossible for only information security professionals to handle them. There is therefore the need to involve end-users by educating them to be aware of threats, and their role in curbing those threats.

Related information security literature was reviewed to establish the business problem theoretically. Previous literature primarily showed the need for more research into the user perspectives and perceptions of information security as a source of information to fine-tune information security arrangements in the organization. Thus, using focus group discussions and open-ended interview guide, data was collected from non-security employees from Takoradi Technical University. The data provided understanding of the employees' present security needs, employee perception of information security, employees' personal security initiative, and level of information security awareness. The key findings in the study suggest that, currently some arrangements have been made to ensure information security; however, there is the need for more non-computer-based arrangements such as physical security and training, and data backup systems.

Further, some of the respondents do not perceive the current arrangements to ensure information security as adequate. How then do the employees make up for the shortfalls?

They take personal initiatives like using passwords, using formal communication

channels for obtaining information which falls outside their domain or function, and seldom reporting any perceived security threats. These personal initiatives seem to be the basis of the employees' self-rating of their level of information security awareness, not some training they have received.

10. Conclusions of the Study

Based on the findings reported, this study draws three conclusions.

First, institutions make efforts, and adopt various security measures. However, the likelihood for such efforts to be independent of end-user input is high. As noted from previous literature, and the findings of the study, the situation causes a mismatch between the information security needs of the employees and the formal efforts.
Second, the extent of the mismatch has an influence on the initiatives taken by employees to close the information security gap. This forms the premise of the third conclusion that, end-users who have some level of information security training are better placed to take initiatives to face the information security gap's risk of widening if formal security arrangements increasingly do not meet the needs of end-users.

Overall, the findings are by no means exhaustive. It may not be an authoritative representation of employee perception of information security. This is because of the number of concepts included in the focus group discussions. Further, to increase generalizability levels, the interview guide could be adapted in the design of a questionnaire for use in a survey with a bigger sample size.

This study however shows that employee security needs and perceptions need to be considered in drawing formal security programmes for organizations.

11. Recommendations

Based on the findings, the study makes the following recommendations.

First, as was observed some of respondents did not use passwords because they used shared computers. Nevertheless, the ICT department or any authorized person could create multiple user accounts for use on that computer. This measure is to eliminate the potential risk of not having a password on an information resource which need not be open.

As a long-term measure, there should be enough computers provided for each Units/Sections/Departments in the Polytechnic, such that the need to share a computer would be eliminated or reduced.

In addition, there should be incentives for staff members whose initiatives i.e., both actions and inactions prevent security threats. This measure is to encourage more people to toe the line of becoming security-conscious.

Yet, the level of awareness and security-consciousness largely depends on training

given by the organization's information security professionals. In order to ensure high information security awareness, there should be regular training for end-users. Continuous bits of information could also be shared via staff email and notice boards to keep staff informed and abreast with current happenings.

References

Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in security management. *Information Management and Computer Security*, *19* (1), 5-24.

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, *18* (4), 226-276.

Ahmed, F., & Siyal, M. Y. (2005). A novel approach for regenerating a private key using password, fingerprint and smart card. *Information Management & Computer Security*, *13* (1), 39-54.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. *Information Management & Computer Security*, *17* (1), 53-63.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, *19* (5), 300-312.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information Security and Risk Management. *Communications of the ACM*, *51*, 64-68.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107* (3), 438-458.

Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, *16* (4), 360-376.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, *16* (5), 484-501.

Crane, S., & Pearson, S. (2011). Security /Trustworthiness Assessment of Platforms. In J. Camenisch, R. Leenes, & D. Sommer (Eds.), *Digital Privacy: PRIME - Privacy and Identity Management for Europe* (p. 464). Berlin-Heidelberg: Springer.

CSI. (2011). *2010/2011 Computer Crime and Security Survey.* New York: Computer Security Institute.

Da Veiga, A. D., & Ellof, J. P. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*, 361-372.

Debar, H., & Viinikka, J. (2006). Security Information Management as an outsourced service. *Information Management and Computer Security*, *14* (5), 417-435.

Desai, M. S., Desai, K. J., & Phelps, L. D. (2012). E-commerce policies and customer privacy: a longitudinal study (2000-2010). *Information Management & Computer Security*, *20* (3), 222244.

Enescu, M., Enescu, M., & Sperdea, N. M. (2011). The Significance of security management: the functions of information security required by organizations. *Economics, Management Financial Markets*, *6* (2), 200-205.

Feruza, S. Y., & Kim, T. -H. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*, *2* (2), 17-31.

Futcher, L., Schroder, C., & von Solms, R. (2010). Information security education in South Africa. *Information Management & Computer Security*, *18* (5), 366-374.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, *19* (4), 216-230.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*, *17* (3), 276-289.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16* (4), 377-397.

Harnesk, D., & Lindstrom, J. (2011). Shaping security behaviours through discipline and agility: Implication for security management. *Information Management and Computer Security*, *19* (4), 262-276.

Hellstrom, T., & Husted, K. (2004). Mapping knowledge and intellectual capital in academic environments. *Journal of Intellectual Capital*, *5* (1), 165-180.

Ifinedo, P. (2007). An empirical study of ERP success evaluations by business and IT managers. *Information Management & Computer Security*, *15* (4), 270-282.

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions: is national culture a differentiator. *Information Management & Computer Security*, *17* (5), 373-387.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security*, *1* (2), 125-143.

Jali, M. Z., Furnell, S. M., & Dowland, P. S. (2010). Assessing image-based authentication techniques in a web-based environment. *Information Management & Computer Security*, *18* (1), 43-53.

Jinks, A. M., & Daniels, R. (1999). Workplace health concerns: a focus group study. *Journal of Management in Medicine*, *13* (2), 95-104.

Johnston, A. C., & Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM*, *52* (1), 126-129.

Kapodistria, H., Mitropoulos, S., & Douligeris, C. (2011). An advanced web attack detection prevention tool. *Information Management & Computer Security*, *19* (5), 280-299.

Kapoor, B., Pandya, P., & Sherif, J. S. (2011). Cryptography: a security pillar of privacy, integrity and authenticity of data communication. *Kubernetes*, *40* (9/10), 1422-1439.

Kreuger, R. A. (1988). *Focus Group: A Practical Guide for Applied Research.* Newbury Park, CA: Sage.

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18* (5), 316-327.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*, 4-13.

Leitao, B. J., & Vergueiro, W. (2000). Using the focus group approach for evaluating customers' opinions: the experience of a Brazilian academic library. *New Library World*, *101* (1154), 60-65.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, *16* (3), 251-270.

Miller, D. R., Harris, S., Harper, A. A., VanDyke, S., & Blask, C. (2011). *Security Information and Event Management (SIEM) Implementation.* New York: McGraw-Hill.

Mitropoulos, S., Patsos, D., & Douligeris, C. (2007). Incident response requirements for distributed security information management systems. *Information Management & Computer Security*, *15* (3), 226-240.

Mow, I. T. (2012). Comparative study and analyses of the status of information security and risk management practices in 3 institutions in Samoa. *Proceedings @ IJITCS* (pp. 1-13). Hong Kong: IMACST.

Nohlberg, M., & Backstrom, J. (2007). User-centered security applied to the development of a management information system. *Information Management & Computer Security*, *15* (5), 372381.

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, *20* (4), 264-280.

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users. *Information Management & Computer Security*, *15* (5), 362-371.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing emails better than others? *Information Management & Computer Security*, *20* (1), 18-28.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in Computing.* Upper Saddle River, NJ: Prentice- Hall.

Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security*, *19* (2), 95-112.

Shoemaker, D. A. (2010). Self-exposure and exposure of the self: informational privacy and the presentation of identity. *Ethics in Information Technology*, *12* (1), 3-15.

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security*, *17* (4), 296-310.

Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticizing the technocratic approach to information security awareness. *Information Management & Computer Security*, *20* (1), 29-38.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly*, *22* (4), 441-469.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems*, *111* (4), 570-588.

Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organizational behaviour. *Information Management & Computer Security*, *20* (1), 39-46.

von Solms, B. (2001). Information Security - a multidimensional discipline. *Computers and Security*, *20* (6), 504-508.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46* (8), 91-95.

Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, *6* (3), 60-70.

Wills, C. E., & Zelijkovic, M. (2011). A personalized approach to web privacy: awareness, attitudes and actions. *Information Management & Computer Security*, *19* (1), 53-73.

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16* (5), 463-483.

Yang, S. S., & Choi, H. (2010). Vulnerability analysis and the practical implications of a server-challenge-based one-time password system. *Information Management & Computer Security, 18* (2), 86-100.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17* (4), 330-340.