IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2347-4599; ISSN(P): 2321-8843
Vol. 3, Issue 11, Nov 2015, 49-60

ASSESSING ORGANISATIONAL INFORMATION SYSTEMS SECURITY BY HUMAN INSIDERS N PRIVATE AND PUBLIC UNVERSITIES IN UGANDA

BUSINGE PHELIX MBABAZI

Lecturer Information Systems Ag. Head of Department Computer and Information Science, Faculty of Techno science, Muni University, Uganda

ABSTRACT

Information system security management is expected to be a high priority for organizational success, given that Information is critical both as input and output of an organization. Hence, there is need to have a secure information system to conduct any business related activities to ensure six objectives of information security: confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing or traceability; and non-repudiation of the information.

This study identified the objectives of information security, key human insider threats which affect information system security of Business organization and the level of information security policy compliance in organizations.

The study was carried out in two Universities one private and another Public University where forty (40) Questionnaires were distributed and the findings showed Institutional data security (protecting company information assets) with mean of 3.79 and Employees (safety, satisfaction, retention) with mean of 3.00 which helps to motivate insider to feel part of organization were given law priority and Respondents also indentified Laptops ranked as number 1 (mean =3.91) as frequently used device in the institution to cause threat on institutional data security followed by Mobile phones ranked as Number 2(mean=3.75).

The study also further discovered that Policies on cyber security (use of social medias e.g. face book) (mean=2.45) was not implemented, Policies on Bring Your Own Device to be used at the Institution (Mean =2.53) was not implemented and Data destruction policies for your Institutional data materials that contain sensitive information (mean=2.52) was not implemented.

The following behaviors were ranked top which need to be worked on; usage of secondary storage devices like flash discs, CD, Hard disks (mean=3.88), Sharing of secondary storage devices like flash discs, CD, Hard disks (Mean=3.48) was also frequent and using of personally owned mobile devices to do office work (mean=3.27) was also ranked among the top behaviors.

KEYWORDS: Information Security; Human Insider Threats; Mobile Devices

INTRODUCTION

Little real-world data is available about the insider threat (Pfleeger, 2008).Recognizing insiders attempting to do something they should not on a corporate or organizational (computer) system is important in cyber and organizational security in general.

"Insider threat" has received considerable attention, and is cited as one of the most serious security problems. Insider threat is considered one of the most difficult problems to deal with because insiders often have information and capabilities not known to management and other stakeholders who can cause serious harm. More real-world data is needed about the insider threat.

Given that Information is critical both as input and output. Hence information security management is of high priority in organization, it's important to have a secure information system to conduct any business related activities to ensure six objectives of information security: confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing or traceability; and non-repudiation of the information (Byrnes and Proctor, 2002))

While information security plays an important role in protecting the data and assets of an organization, we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organizations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government and organizations.

Information security plays an important role in protecting the assets of an organization. As no single formula can guarantee 100% security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted given the increased usage of Mobile device by insiders.

Information security management in ISO17799 is based on risk management. The latter is defined in the standard as the "Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost" (ISO/IEC, 2000).

Modern information systems are confronted by a variety of threats. Although attacks originating from outside, such as hacking attempts or viruses, have gained a lot of publicity, insider threats pose a significantly greater level of risk (Schultz, 2002). Unfortunately, the controls and tools that are used for the protection of the IS from externally initiated attacks (e.g. firewalls and intrusion detection systems) are not effective in detaining insider threat, as the latter requires a different approach (Porter, 2003; Lee and Lee, 2002; Schultz, 2002).

Problem Statement

Most Issues related to institutional data security are happening due to people factor such as accidental disclosure, insider curiosity, data breach by insider, data breach by outsider physical intrusion, unauthorized intrusion of network system (NRC 1997); more especially, the human insiders who legitimately access institutional data are a greater threat to institutional data security either intentionally, inadvertently or accidentally (Richardson, 2009) to manipulate, corrupt or leak institutional data and is therefore more detrimental to the existence of the institution. Therefore there is need for institutions to clearly indentify the threats and also ascertain if the human insiders comply to the institutional policies so that they can address those threats.

Main Objective

The main objective was to identity of threats on institutional data security posed by human insiders and ascertains information System security policy compliance by human insiders in the Institutions

Specific Objectives

The specific objectives of the study were.

- To identify threats on institutional data security posed by human insiders.
- To ascertain information System security policy compliance by human insiders in the Institutions

Significance of the Study

The study clearly shows organization's priority in terms of Financials, Customer satisfaction, Innovation (the ability to create new products and/or business processes), Information Technology (using the best, most modern technologies), Institutional data security (protecting company information assets), Employees (safety, satisfaction, retention).This study also gives a clear picture of the possible threats on institutional data security by human insiders and the level of information security policy compliance by institutions.

RELATED LITERATURE

Insider Threat

An Insider is defined as an individual with privileged access to an IT system (Richardson, 2008), Nick (2010) insider threat is an individual and, more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust in or with the infrastructure or institution being targeted.

According to Greitzer and Hohimer, (2011)The insider threat refers to harmful acts that trusted insiders might carry out, such as something that causes harm to the organization or an unauthorized act that benefits the individual. Information "leakage," espionage, and sabotage involving computers and computer networks are the most notable examples of insider threats, and these acts are among the most pressing cyber-security challenges that threaten government and private-sector information infrastructures. The insider threat is manifested when human behaviors depart from established policies, regardless of whether they result from malice, disregard, or ignorance. Due to the legitimacy and trust the insiders enjoy, this type of crime is difficult to detect and mitigate before the occurrence..

Several industry reports indicate that both intentional and unintentional insider threats are considered as one of the top ranked threats to information security over the past decade (Richardson, 2009). For instance, according to the 2004 E-crime Watch Survey (CSO, 2004), 36 Percent of the respondents experienced unauthorized access by insiders. There is an increasing trend as the more survey reported that 49 Percent of the respondents' experienced malicious insider attacks (CSO, 2004).

Information System Security Goals

According to Arumugam (2013) a computer-based system has three primary valuable assets to protect; they are the hardware, software and data assets. A secure system accomplishes its task with no unintended side effects. The computer security threats which exploit the vulnerabilities of computer assets are interception, interruption, modification

and fabrication. The fundamental security goals which ensure that the hardware, software and data assets are not compromised by the threats include Confidentiality (C), Integrity (I), and Availability (A) Legitimate Use (L), Auditing Or Traceability (A/T),Non-repudiation(NR).

Qingxiong Et al (2008 effective information security system also must have the following six objectives: confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing or traceability; and non-repudiation. If these objectives could be achieved, it would alleviate most of the information security concerns.

According to Arumugam (2013) the fundamental security goals which ensure that the hardware, software and data assets are not compromised by the threats are:

Confidentiality

Providing access privileges to users in accessing the data. It involves making information accessible to only authorized parties, or restricting information access to unauthorized parties.

Integrity

Restricting alteration rights to the original data. For example Transmitting information over the Internet (or any other network) is similar to sending a package by mail. The package may travel across numerous trusted and untrusted networks before reaching its final destination. It is possible for the data to be intercepted and modified while in transit. This modification could be the work of a hacker, network administrator, disgruntled employee, government agents or corporate business intelligence gatherer; it could also be unintentional.

Availability

Data accessible and operational whenever it is required. Availability means that systems, data, and other resources are usable when needed despite subsystem outages and environmental disruptions

Legitimate Use

Includes identification, authorization, and authentication. Identification involves a process of a user positively identifying itself (human or machine) to the host (server) that it wishes to conduct a transaction with. The most common method for establishing identity is by means of username and password. The response to identification is authentication. Without authentication, it is possible for the system to be accessed by an impersonator. Authentication needs to work both ways: for users to authenticate the server they are contacting, and for servers to identify their clients. Authentication usually requires the entity that presents its identity to confirm it either with something the client knows (e.g. password or PIN), something the client has (e.g. a smart card, identity card) or something the client is (biometrics: finger print or retinal scan). Biometric authentication has been proven to be the most precise way of authenticating a user's identity.

Auditing or Traceability

Process of examining the transactions: From an accounting perspective, auditing is the process of officially examining accounts. Similarly, in an e-business security context, auditing is the process of examining transactions. Trust is enhanced if users can be assured that transactions can be traced from origin to completion. If there is a discrepancy or

dispute, it will be possible to work back through each step in the process to determine where the problem occurred and, probably, who is responsible. Order confirmation, receipts, sales slips, etc. are examples of documents that enable traceability. In a well-secured system, it should be possible to trace and recreate transactions, including every subcomponent, after they are done. An effective auditing system should be able to produce records of users, activities, applications used, system settings that have been varied, etc., together with time stamps so that complete transactions can be reconstructed.

Non-Repudiation

ability of an originator or recipient of a transaction to prove to a third party that their counterpart did in fact take the action in question. Thus the sender of a message should be able to prove to a third party that the intended recipient got the message and the recipient should be able to prove to a third party that the originator did actually send the message. This requirement proves useful to verify claims by the parties concerned and to apportion responsibility is cases of liability.

Information Security in the Workplace

Considerable research has focused on information security-related behavior in the workplace. Generally, workplace threats are divided into those external to the organization and those internal to the organization. Because these two types of threats often stem from different motivations, research studies usually treat them separately. Insider threats have also been further defined to include human versus nonhuman and accidental versus intentional.

User errors and negligence are some of the most common accidental errors and are considered one of the worst threats to information security (Whitman and Mattord 2004). Although reasons for user errors are numerous, simple lack of awareness of the importance of information security is an obvious factor.

Institutional Data Threats

Recent studies suggest that the broad spectrum of organizational threats could be categorized into five levels, in the increasing order of sophistication (NRC 1997):

- Accidental disclosure: Employees unintentionally discloses for example institution information to others, e.g. email message sent to wrong address or an information leak through peer-to-peer file sharing.
- Insider curiosity: an insider with data access privilege pries upon a Employees records out of curiosity or for their own purpose, e.g. a nurse accessing information about a fellow employee to determine possibility of sexually transmitted disease in colleague; or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting to media.
- Data breach by insider: insiders who access Employees information and transmit to outsiders for profit or taking revenge on employees.
- Data breach by outsider with physical intrusion: an outsider who enters the physical facility either by coercion or taking revenge on Employees.

- Unauthorized intrusion of network system: an outsider, including former vengeful employees, or hackers who intrude into organization‘s network system from outside and gain access to institutional information or render the system inoperable.

Human Insider Threat on Data Security

There is much debate on the insider threat but, compared to outsider attacks, there is far less factual data on which to base analysis and conclusions. In the USA, the National Infrastructure Advisory Council (NIAC, 2008) highlights that awareness and mitigation of insider threats varies greatly among companies and sectors and is often dealt with poorly.The BERR (2008) concludes that in the UK many organizations are still not doing enough to protect themselves and their customers’ information (including some areas significant for the insider threat):

- 52 Percent do not carry out any formal security risk assessment.
- 67 Percent do nothing to prevent confidential data leaving on USB sticks, laptops and other mobile devices.
- 78 Percent of companies had computers with unencrypted hard discs stolen.
- 84 Percent of companies do not scan outgoing email for confidential data.

Colwill (2009) affirms that most physical and electronic attacks can be assisted or conducted by an insider but some attacks can only be committed by insiders, such as the unauthorized release of proprietary information or the sabotage of assets that only employees can access.

Silic and Back, 2013, reiterates that the Increase use of Mobile devices have a huge consequences in the way we treat information, as smart phones are bringing another dimension to information processing: video, ecommerce, location based services, photo sharing and social media. The number of new services, apps and tools is increasing and every day we are seeing a new mobile based service or new application appearing

Greitzer et al (2010), identified One might legitimately ask: Can we pick up the trail before the fact, providing time to intervene and prevent an insider attack? Why is this so hard? There are several reasons why development and deployment of approaches to addressing insider threat, particularly proactive approaches, are so challenging:

- The lack of sufficient real-world data that has "ground truth" enabling adequate scientific verification and validation of proposed solutions;
- The difficulty in distinguishing between malicious insider behavior and what can be described as normal or legitimate behavior (since we generally don't have a good understanding of normal versus anomalous behaviors and how these manifest themselves in the data);
- The potential quantity of data, and the resultant number of "associations" or relationships that may emerge produce enormous scalability challenges;
- Despite ample evidence suggesting that in a preponderance of cases, the perpetrator exhibited observable "concerning behaviors" in advance of the exploit, there has been almost no attempt to address such human factors by researchers and developers of technologies/ tools to support insider threat analysis.

According to Ponemon(2012) it identified some 10 risky practices employees (human Insiders) routinely engage as follows;

- Connecting computers to the Internet through an insecure wireless network.
- Not deleting information on their computer when no longer necessary.
- Sharing passwords with others.
- Reusing the same password and username on different websites.
- Using generic USB drives not encrypted or safeguarded by other means.
- Leaving computers unattended when outside the workplace.
- Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
- Working on a laptop when traveling and not using a privacy screen.
- Carrying unnecessary sensitive information on a laptop when traveling.
- Using personally owned mobile devices that connect to their organization's network.

METHODOLOGY

We applied Survey method in this study of research with the aim of gathering the connected matter with information of our research; we had to prepare a questionnaire for both administrative staff and ICT Technical staff members.

Fouty (40) Questionnaires were distributed in two Universities, one private and one public, 20 Questionnaires were each University and 33 Questionnaires were returned.

Preliminary Findings

Table 1: Respondents

	Institution Characteristics	
Category of Institution		**Frequency**
	Private	18
	Public	15
	Total	**33**

A total of 33 staff members were sampled and PRIVATE was represented by 18 and Public University by 15.

Institutional Priority

Table 2: Institutional Priority

	Institutional Priority	Institution	Mean	Interpretation	Mean	Interpretation	Ranking
1.	Financials	**Private**	4.06	Priority	3.97	Priority	**4**
		Public	3.87	Priority			
2.	Customer satisfaction	**Private**	3.61	Priority	4.03	Priority	**2**
		Public	4.57	High Priority			
3.	Innovation (the ability to create new products and/or	**Private**	3.83	Priority	4.00	Priority	**3**
		Public	4.20	Priority			

	business processes)						
4.	Information Technology (using the best, most modern technologies)	**Private**	4.11	Priority	4.30	Priority	**1**
		Public	4.53	High Priority			
5.	Institutional data security (protecting company information assets)	**Private**	3.39	Partly Priority	3.79	Priority	**5**
		Public	4.27	High Priority			
6.	Employees (safety, satisfaction, retention)	**Private**	2.56	Not Priority	3.00	Partly Priority	**6**
		Public	3.53	Priority			

Despite Information Technology (using the best, most modern technologies) with average of 4.30 was given high priority in institutions, the key issues which can be a loop hall to institutional security were the least i.e Institutional data security (protecting company information assets) with 3.79 which can help in ensuring organizational information security and Employees (safety, satisfaction, retention) with 3.00 which helps to motivate insider to feel part of organization.

Frequently used device

Table 3: Frequently used Device

Frequently Used Device in The Institution to Cause Threat on Institutional Data Security:		Institution	Mean	Interpretation	Mean	Interpretation	Ranking
1.	Mobile Phone	Private	3.83	Frequently Used	3.75	Frequently Used	**2**
		Public	3.64	Frequently Used			
2.	Laptop	Private	3.72	Frequently Used	3.91	Frequently Used	**1**
		Public	4.13	Frequently Used			
3.	I pad	Private	3.00	Used	2.91	Used	**5**
		Public	2.80	Used			
4.	Workstation	Private	3.35	Used	3.43	Frequently Used	**4**
		Public	3.54	Frequently Used			
5.	Servers	Private	3.72	Frequently Used	3.48	Frequently Used	**3**
		Public	3.20	Used			

The table above clearly shows that the respondents indentified Laptops ranked as number 1 (mean =3.91)as frequently used device in the institution to cause threat on institutional data security which means there must be serious measures to control usage of laptops in organization and this was followed by Mobile phones ranked as Number 2(mean=3.75) :

Information Security Policy Compliance by Organizations

Table 4: Information Security Policy Compliance

	Information Security Policy	Institution	Mean	Interpretation	Mean	Interpretation	Rank
1.	Back-ups storage policies for your Institutional data materials that contain sensitive Information.	Private	2.94	Partly Implemented	3.12	Partly Implemented	6
		Public	3.33	Partly Implemented			
2.	Offsite storage policies for your Institutional data materials that contain sensitive Information.	Private	2.61	Partly Implemented	2.52	Not Implemented	15
		Public	2.4	Not			

				Implemented			
3.	Data classification policies for your Institutional data materials that contain sensitive information	Private	3.11	Partly Implemented	2.97	Partly Implemented	7
		Public	2.80	Partly Implemented			
4.	Data retention policies for your Institutional data materials that contain sensitive information	Private	2.78	Partly Implemented	2.85	Partly Implemented	11
		Public	2.93	Partly Implemented			
5.	Data destruction policies for your Institutional data materials that contain sensitive information	Private	2.94	Partly Implemented	2.52	Not Implemented	16
		Public	1.92	Not Implemented			
6.	Policies on access control, authentication and authorization practices for using the Institutional Information Systems	Private	2.89	Partly Implemented	2.97	Partly Implemented	8
		Public	3.07	Partly Implemented			
7.	Policies on protection of Institutional IS assets to protect your Institutional hardware, software, data and people.	Private	3.17	Partly Implemented	3.33	Partly Implemented	2
		Public	3.53	Implemented			
8.	Polices on reporting of Information Systems security events	Private	2.78	Partly Implemented	2.88	Partly Implemented	10
		Public	3.00	Partly Implemented			
9.	Polices on response of Information Systems security events	Private	2.76	Partly Implemented	2.94	Partly Implemented	9
		Public	3.13	Partly Implemented			
10	Policies on acceptable use of wireless devices in your Institutional such as laptops and hand phones.	Private	3.39	Partly Implemented	3.26	Partly Implemented	3
		Public	3.08	Partly Implemented			
11	Policies on acceptable use of workstations in your Institutional such as personal computers.	Private	3.33	Partly Implemented	3.18	Partly Implemented	4
		Public	3.00	Partly Implemented			
12	Policies on acceptable use of e-mails in your Institutional	Private	3.24	Partly Implemented	3.41	Implemented	1
		Public	3.60	Implemented			
13	Policies on sharing of Institutional data via the network	Private	2.89	Partly Implemented	3.15	Partly Implemented	5
		Public	3.47	Implemented			
14	Policies on storing of Institutional data via network	Private	2.94	Partly Implemented	2.84	Partly Implemented	12
		Public	2.73	Partly Implemented			
15	Policies on cyber security (use of social medias e.g. face book) as far as Institutional data security is concerned	Private	2.83	Partly Implemented	2.45	Not Implemented	17
		Public	2.00	Not Implemented			
16	Policies on regular review of the different information security policies	Private	3.06	Partly Implemented	2.79	Partly Implemented	13
		Public	2.47	Not Implemented			
17	Policies on Bring Your Own Device to be used at the Institution	Private	2.82	Partly Implemented	2.53	Not Impleme	14

		Public	2.20	Not Implemented		nted	

The study showed that most of the policies are partly implemented and Policies on cyber security (use of social medias e.g. face book) as far as Institutional data security is concerned (mean=2.45) was not implemented, Policies on Bring Your Own Device to be used at the Institution (Mean =2.53) was not implemented and Data destruction policies for your Institutional data materials that contain sensitive information (mean=2.52) was not implemented which is dangerous to the organizations since these can be the means which can be a threat to the Institutional data security by human insiders either intentionally or unintentionally.

Threats Posed on Information System Security by Insiders

Table 5: Threats Posed on Information System Security by Insiders

	Human Insider Threat	Institution	Mean	Interpretation	Mean	Interpretation	Rank
1.	Insiders who access Employees information and transmit to outsiders for profit or taking revenge on others	Private	2.39	Not frequent	2.09	Not frequent	**15**
		Public	1.73	Not frequent at all			
2.	Unintentionally disclose of information to others, e.g. email message sent to wrong address or an information leak through peer-to-peer file sharing	Private	2.33	Not frequent	2.21	Not frequent	**14**
		Public	2.07	Not frequent			
3.	Connecting computers to the Internet through an insecure wireless network	Private	2.24	Not frequent	2.25	Not frequent	**13**
		Public	2.27	Not frequent			
4.	Deleting information on their computer when no longer necessary.	Private	2.83	Sometimes	3.03	Sometimes	**4**
		Public	3.27	Sometimes			
5.	Deleting information on their computer accidently.	Private	2.88	Sometimes	2.81	Sometimes	**6**
		Public	2.73	Sometimes			
6.	Sharing of passwords with other staff members	Private	3.17	Sometimes	2.73	Sometimes	**8**
		Public	2.20	Not frequent			
7.	Reusing the same password and username on different logins	Private	2.67	Sometimes	2.57	Sometimes	**11**
		Public	2.42	Not frequent			
8.	Using of secondary storage devices like flash discs, CD, Hard disks.	Private	3.39	Sometimes	3.88	Frequent	**1**
		Public	4.47	Very Frequent			
9.	Sharing of secondary storage devices like flash discs, CD, Hard disks.	Private	3.06	Sometimes	3.48	Frequent	**2**
		Public	4.00	Frequent			
10.	Losing of Secondary storage devices like flash disks, CD, Hard disk, floppy.	Private	2.61	Sometimes	2.64	Sometimes	**10**
		Public	2.67	Sometimes			
11.	Leaving computers unattended to.	Private	2.82	Sometimes	2.78	Sometimes	**7**
		Public	2.73	Sometimes			
12.	Failing to have automatic lock of the screen savers	Private	2.53	Not frequent	3.00	Sometimes	**5**
		Public	3.50	Frequent			
13.	Working on a mobile device e.g. laptop while traveling	Private	2.33	Not frequent	2.42	Not frequent	**12**
		Public	2.53	Not frequent			
14.	Loosing mobile devices e.g. laptops, IPad	Private	2.78	Sometimes	2.70	Sometimes	**9**
		Public	2.60	Sometimes			
15.	Using of personally owned mobile devices to do office work	Private	3.11	Sometimes	3.27	Sometimes	**3**
		Public	3.47	Frequent			

The results of the table above showed that using of secondary storage devices like flash discs, CD, Hard

disks(mean=3.88) was frequent which can be one of the source of leakage of Institutional data either intentionally or unintentionally, Sharing of secondary storage devices like flash discs, CD, Hard disks(Mean=3.48) was also frequent which can also be a threat to institutional data security, Using of personally owned mobile devices to do office work(mean=3.27) was also ranked among the top behaviors which is a threat to institutional data security if there is no clear BYOD policy.

On top of the above threats, Failing to have automatic lock of the screen savers, deleting information on their computer when no longer necessary, deleting information on their computer accidently and leaving computers unattended to were ranked as some of the common behaviors which can pose a threat to institutional data security.

Future Work

Based on the above findings, the author recommend further investigation on the current mitigation measure used by institutions in mitigating human insider threats on institutional data security

CONCLUSIONS

The study found out that Institutional data security (protecting company information assets) with mean of 3.79 which can help in ensuring organizational information security was given a low priority and Employees (safety, satisfaction, retention) with mean of 3.00 which helps to motivate insider to feel part of organization was also given law priority.

Respondents also indentified Laptops ranked as number 1 (mean =3.91)as frequently used device in the institution to cause threat on institutional data security which means there must be serious measures to control usage of laptops in organization and this was followed by Mobile phones ranked as Number 2(mean=3.75) :

The study also further discovered that Policies on cyber security (use of social medias e.g. face book) as far as Institutional data security was concerned (mean=2.45) was not implemented, Policies on Bring Your Own Device to be used at the Institution (Mean =2.53) was not implemented and Data destruction policies for your Institutional data materials that contain sensitive information (mean=2.52) was not implemented which can easily be a source of leakage of sensitive institutional data.

The following behaviours were ranked top which need to be worked on; usage of secondary storage devices like flash discs, CD, Hard disks (mean=3.88) was frequent which can be one of the source of leakage of Institutional data, Sharing of secondary storage devices like flash discs, CD, Hard disks (Mean=3.48) was also frequent and using of personally owned mobile devices to do office work (mean=3.27) is also ranked among the top behaviors

The major limitation to this study was the low response rate, which is synonymous with survey studies.

ACKNOWLEDGEMENTS

The authors would like to thank Public University for giving me permission to collect data from the staff members and Private University management for allowing me use the University as my Unit of analysis. The authors also wish to thank all respondents who gave of their time to participate in our survey are also appreciated. I cannot forget my family my dear wife Ms.Namugabo Lydia Abwooli, my son Kisembo Hope Innocent Abwooli , my daughter Ainomugisa Praise

abwooli for their support while we were doing this work and Dr. Joseph Kizito Bada for his guidance.

REFERENCES

1. BERR. Department for business Enterprise and regulatory Reform (BERR) information security breaches survey, 2008
2. Byrnes, F. and Proctor, P. (2002), "Information security must balance business objectives
3. Carl Colwill , Human factors in information security: The insider threat e Who can you trust these days?,2009.
4. CSO Magazine. (2004). E-Crime Watch Survey, CXO Media Inc.
5. F.L. Greitzer and D.A. Frincke,(2010) "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat," in: Christian
6. ISO/IEC (2000), "Information technology – Code of practice for information security management", ISO/IEC 17799:2000(E), Geneva, Switzerland
7. Lee, J. and Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2): 57-63.
8. Mario Silic and Andrea Back, Factors impacting information governance in the mobile device dual-use context, Records Management Journal Vol. 23 No. 2, 2013
9. NIAC. HMG IA standard No. 1, technical risk assessment part 1 (Issue 3.2); October 2008.
10. *Nick Catrantzos*: Tackling the Insider Threat, 2010:
11. NRC National Research Council (1997) ―For the Record: Protecting Electronic Health Information
12. Pfleeger C., Pfleeger S. (2003), 'Security in Computing', Third Edition, Prentice Hall,
13. Ponemon Institute, the Human Factor in Data Protection, 2012
14. Porter, D. (2003). Insider fraud: Spotting the wolf in sheep's clothing. *Computer Fraud & Security*, 2003(4): 12-15.
15. Qingxiong Ma, Allen C. Johnston, J. Michael Pearson (2008) Information security management objectives and practices: a parsimonious framework
16. Richardson, R. (2009). CSI Computer Crime & Security Survey. Computer Security Institute
17. Schultz, E.E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security*, 21(6): 526-531
18. Whitman, M.E., and Mattord, H.J. 2004. "Designing and Teaching Information Security Curriculum," *Proceedings of the InfoSecCD Conference*, M.E. Whitman (ed.), Kennesaw, GA: ACM, pp. 1-7.