International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
www.allsubjectjournal.com
Volume 3; Issue 5; May 2016; Page No. 59-66

Unintentional human insider threats mitigation measures in universities in Uganda

[1] Businge Phelix Mbabazi, [2] Jehopio Peterand [3] JWF Muwanga – Zake

[1] PhD MIS candidate, Kampala International University, School of Computing and Information Technology
[2, 3] Senior Lecturer Kampala International University School of Computing and Information Technology

Abstract
The purpose of this research paper to indentify the unintentional human insider threats and assess the various unintentional Human Insider threats mitigation measures currently used in universities in Uganda. It also intends to know the mitigation measures are actually being implemented in the universities in Uganda. The primary data was collected by using survey method. Sampling was all from ICT Staff members and the various heads of Departments who are in charge of handling institutional data. The questionnaires were distributed to 212 respondents from conveniently selected respondents from different Nine (9) Universities in Uganda. Reliability and validity of the constructs tests were carried out and all were found to be above the recommended values and Descriptive Statistics and coefficient of Variation was used to analyze these constructs.

The study found out that sharing of secondary storage devices like flash discs, CD, Hard disks, Losing of Secondary storage devices like flash disks, CD, Hard and Working on a mobile device e.g. Laptop while travelling, Leaving computers unattended to were the top ranked insider threats and Usability of security tools were being implemented while Technological measures, Security training and awareness, Deterrence measures were partly implemented and Motivation measures, and Time pressure and Workload were sometimes implemented.

Its recommend to further investigate on the other unintentional mitigation measure which can be used in mitigating other insider threats on institutional data security for example hackers and none human threats to information security such natural disasters and systems failures.

Keywords: Insider threats, Unintentional Human Insider threats, Mitigation Measures, Universities

1. Introduction

1.1 Insider Threats

Information system security threats can be categorized into three (3), Intentional threats, Unintentional threats and natural threats. Insider attack is the intentional misuse of computer systems by users who are authorized to access those systems and networks. Parallel to this definition, computer abuse and fraud are considered as the most common intentional insider threats to information security. According to Miller and Maxim (2015) [26] insider threats differ and could be classified into three types: malicious insiders who deliberately steal information or cause damage; insiders who are unwittingly exploited by external parties, and; insiders who are careless and make unintended mistakes.

1.2 Handling human insider threats

Organizations are expected to take the following steps: Create awareness among employees and other insiders about the need to spend more time and effort on data protection activities; Ensure data protection policies address areas where an organization is most vulnerable to a data breach; Investigate governance and technology solutions that are both efficient and cost effective; Make sure those who are given privileged user status are knowledgeable about the risks; Require immediate notification if a mobile device containing sensitive and confidential information is lost or stolen, and; Create policies for the use of social media in the workplace.

1.3 Challenges in trying to mitigate human insider threats

According to Miller & Maxim (2015) [26], Institutions face common challenges when attempting to reduce their risk of human insider security breaches namely such as ineffective management of privileged users and inappropriate role and entitlement assignment. Other challenges include; Poor overall identity governance; Poor information classification and policy enforcement; Inadequate auditing; Audit log complexity; Reactive response, and; No comprehensive written acceptable use policies.

This study aimed at assessing the Human insider threats mitigation measures which are currently used in Universities in Uganda.

1.4 Information Security in the Workplace

According to Yayla & Alper (2010) [35] as organizations are becoming more dependent on information technology, the emphasis on information security is getting more significant. Threats to information security have several dimensions including internal versus. External, human versus. Non-human, and accidental versus.

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 (Loch *et al*. 1992) [20].

User errors and negligence are some of the most common accidental errors and are considered one of the worst threats to information security (Whitman & Mattord 2004) [34]. Although reasons for user errors are numerous, simple lack of awareness of the importance of information security is an obvious factor.

1.5 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) [22]: 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 and 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.

1.6 Unintentional human Insider Threats to Institutional Data Security

User errors and negligence are arguably the two most common unintentional insider threats. Whitman (2004) [34] considers "act of human failures or error" as one of the most severe threats to information security. Some of the underlying reasons behind user errors are lack of experience in utilizing security tools, complexity of the security tools, and job stress due to time pressure and workload. On the other hand, although reasons behind negligence are complex, lack of awareness and motivation to use security tools due to their performance hindering characteristics can be considered as important factors. Thus, in this section, we propose to mitigate user error and negligence through five mechanisms: motivation, training, usability of security tools, time and workload pressure, and awareness.

Motivation

Several studies in the IS literature emphasized the positive effect of usefulness on technology acceptance (Davis *et al*., 1989; Taylor & Todd, 1995b) [10, 32]. However, computer security tools are almost never considered from the performance enhancing perspective. In contrary, users consider computer security tools as performance restraining, since encrypting e-mails or managing secure passwords may require extra time, or using firewalls may slow down computer systems. In other words, within the context of security tools, extrinsic rewards of the behavior (e.g., performance increase) become relatively insignificant. Therefore, unless users are intrinsically motivated, successful adoption and usage of computer security tools is unlikely. Similar to these arguments, it's said that reported that apathy has negative effect on the level of precautions taken by users to secure their computers and adhere with security policies.

Training

Training of employees is considered as one of the common methods to ensure their compliance with security policies (Puhakainen & Siponen, 2010) [23]. The positive effect of training to mitigate unintentional insider threats can be categorized in two groups. Firstly, training can increase users' ability to interact with software programs (Nelson and Chenney, 1987) [21]. User skills are often considered as important determinants of intentions and behaviour. For instance, a considerably stream of research based on the Theory of Planned Behaviour (TPB) investigated computer users' intentions. The Perceived Behavioural Control (PBC) construct in TPB captures the perceived ease or difficulty of performing the behaviour.

Secondly, training can have a direct effect on technology usage. During training programs, user would have the opportunity to replicate instructor's behaviors and to engage in trial and error activities.

Usability of Security Tools

The effect of usability on unintentional insider threats is twofold. The first effect is in terms of users' intentions to use existing security tools. Intentions to use computer systems has long been investigated in the IS literature. The Technology Acceptance Model (TAM) (Davis, 1989) [10] captures usability with the Perceived Ease of Use (PEOU) construct. It refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989) [10].

The second effect of usability on unintentional threats is in terms of preventing erroneous use in security technologies. This concept is introduced to IS literature by Saltzer and Schroeder (1975) [27] as Psychological Acceptability (PA). PA is one of the eight specified design principles for constructing secure computer systems, and it focuses on designing human interfaces that are easy to use in order to prevent user errors.

Deterrence Measures

Deterrent factors are considered passive administrative countermeasures; hence, their effectiveness depends completely on individuals (Straub and Welke, 1998) [30]. Awareness programs and policies/guidelines that specify proper use of computer systems are two of the most effective deterrence measures (Straub & Nance, 1990) [31]. Studies in the information systems (IS) literature found empirical support in favor of the effectiveness of deterrence measures (Kankanhalli *et al*., 2003; [16]. However, in order to be effective, deterrence measures should communicate disciplinary actions that will be exercised when perpetrators are identified (Blumstein, 1978) [3]. For instance, D'Arcy *et al*. (2009) [9] reported that perceived certainty and perceived severity of sanctions have negative effect on IS misuse intentions. Its argued that disciplinary action beyond dismissal, for example prosecution, should be considered when a malicious insider has been caught as not only does this prevent that person from simply going to another organization and potentially committing a crime there, but it also demonstrates commitment by the organization to pursue perpetrators of these crimes, which sends a strong deterrence message to other people in the organization.

Technology-based Control

Technology-based controls can be used both for prevention and detection purposes (Baskerville, 1988) [2]. The aim of preventive control is towards reducing possible threats (Baskerville, 1988) [2], mostly by controlling unauthorized access. Detective controls, on the other hand, are purposeful investigation of unauthorized activity, and based on examination of irregularities in system activities, as in the case of intrusion detection systems. Technology-based detective controls can be considered as the second line of defence after preventive controls, and they are designed to minimize the harm caused by threats by identifying security incident occurrences. In their study, Straub and Nance (1990) [31] reported that around 50percent of the detected computer abuses are discovered by system controls, and 16percent of them discovered by purposeful investigation.

Some of the most common technology-based preventive and detective controls are passwords, firewalls, connection security, and cryptography (Haugen & Selin, 1999) [13]. Its postulates that password based authentication is one of the persuasive technologies that can be implemented as a control mechanism. He further argues that although passwords are not as secure as biometric systems, they can be made strong enough for less critical processes. Similar to passwords, firewalls have become one of the most visible security technologies used in organizations (Brussin, 2002) [6]. Intrusion detection systems are also considered as effective detective controls since these tools are utilized not only to detect attacks but also to identify and analyze attack trends (Einwechter, 2002) [11]. Some of the more advanced computer-based controls that can be implemented are public key infrastructures, certificate authorities, and vulnerability assessment (Chokhani, 2002) [8].

Time Pressure and Workload

Environmental conditions such as heavy and prolonged workload and constant time pressure are considered as major sources of stress and fatigue. The effect of emotional arouses on performance has first been investigated by Yerkes & Dudson (1908) [36]. Their well-known inverted U-shaped relationship between arousal and performance was named as Y-D Law in psychology. This law postulates that both low and high arousal levels restrain performance. Later in the literature, this law has been utilized in several experimental studies by psychologists to investigate behavioral and cognitive consequences of such emotional arouses on individuals performance.

Security Awareness

User negligence is a critical factor in the information security context. One way of fighting with negligence is creating awareness among users (Spurling, 1995; Thompson and von Solms, 1998) [28, 33]. The awareness programs have two main objectives; a) making employees aware of procedures, rules and regulation stated in the security policy, and b) making employees aware of security concerns. Increasing users' awareness about security threats and computer-based controls such as authentications and antivirus systems will help them understand the severity of the threats and also increase utilization of these control mechanisms. However, given their importance, awareness programs constitute approximately 1percent of security budgets in organizations.

Employees can become detection instruments of the organization by getting familiar with danger signals through awareness programs. Moreover, awareness of employees can have positive effect on their beliefs and an attitude towards compliance with Institutional data security policies as well as their perceived certainty and severity of sanctions (Bulgurcu *et al*., 2010; D'Arcy *et al*. 2009) [7, 9].

2. Methodology

The study applied Survey method 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. This study targeted 450 population comprising of Heads of Department and ICT Technical Staff members, of the 450 population, 135 Technical ICT staff members as well as 315 Heads of Department in selected educational institutions in Uganda from Two (2) public degree awarding institutions namely and seven (7) from January 2014-August 2015. These Universities were selected from Kampala region since they share the same work environment and the Two Universities were selected to have a representative of the remote area work environment

Using slave's formula above from the population of 450, the sample size calculated was 212 respondents.

The sample was taken from each category or cluster and was calculated using the sampling fraction formula below to arrive at the minimum sample size.

Equation 1 Sampling Fraction

$$\text{Sampling fraction} = \frac{\text{actual sample size}}{\text{total population}}$$

Sampling fraction=212/450

Sampling fraction= 0.471

The sample size for each stratum was later multiplied by the sampling fraction value of 0.471 to get the actual sample size of each stratum.

Table 1: Population and Sample size

Category	Population	Sample Size
Technical IT Staff members	135	64
Administrative Staff	315	148
Total	450	212

The researcher used questionnaire to collect data from the respondents. Questionnaires was used because the sample size was large enough thus they provide the advantage of being more reliable and applicable under survey design. The method was also preferred for its merits as advanced by (Gillham, 2000) [12], which include management of resources, distance, cost and time. In this situation the measurement of constructs in this case therefore was done using Likert's measuring scale and thus the levels of the constructs were estimated basing on the response modes and scoring system of a rage of five (5) or four (4) where applicable where applicable.

The data was collected through a structured questionnaire and was coded and entered into the computer system and statistically treated using the special package for social scientists (SPSS). Frequencies and percentage distributions were used to analyze data on the respondent's profile and the results were presented inform of tables.

3. Findings

Table 2: The Unintentional Human Insider Threats

1.	Human Insider Threat	Mean	Std. Deviation	coefficient of variation	Interpretation
2.	Sharing of secondary storage devices like flash discs, CD, Hard disks.	3.8	1.162	30.58	Frequent
3.	Losing of Secondary storage devices like flash disks, CD, Hard disk, floppy.	3.2	1.17	36.56	Sometimes Frequent
4.	Working on a mobile device e.g. laptop while traveling	3.1	1.161	37.45	Sometimes Frequent
5.	Leaving computers unattended to.	2.9	1.099	37.9	Sometimes Frequent
6.	Deleting information on their computer accidently.	2.4	1.084	45.17	Not Frequent
7.	Reusing the same password and username on different logins	2.2	1.157	52.59	Not Frequent
8.	Sharing of passwords with other staff members	2.3	1.246	54.17	Not Frequent
Mean		2.84	1.154	42.06	Sometimes Frequent

According to the data obtained from Institutional Employees above from the field the following risky behaviours were ranked among the top frequently happening: Sharing of secondary storage devices like flash discs, CD, Hard disks of coefficient of variation of 30.58percent (mean=3.8), Losing of Secondary storage devices like flash disks, CD, Hard disk, floppy of coefficient of variation of 35.10 percent (mean=3) and Working on a mobile device e.g. Laptop while travelling, Leaving computers unattended to, Deleting information on their computer accidently were among the top unintentional behaviors practiced by institutional employees in institutions which are one of the sources of leakage of Institutional data either intentionally or unintentionally.

Current Unintentional Human Insider threats Mitigation Measures

Table 3: Deterrence mitigation measures

A1	*Deterrence measures*	*Mean*	*Std. Deviation*	*coefficient of variation*	*Interpretation*
1.1	Procedures with regard to outsourcing any institutional Information Systems service or activities.	3.18	1.109	34.9	Partly Implemented
1.2	Procedures for handling Institutional sensitive data to prevent unauthorized disclosure or misuse by those who handle it.	3.31	1.224	37.0	Partly Implemented
1.3	Procedures on the intellectual property rights and copyrights in controlling and protecting any digital works or resources for the Institution.	3.04	1.126	37.0	Partly Implemented
1.4	Dismissal of the Employees who have committed offence	3.5	1.318	37.7	Implemented
1.5	Surprise system audits to detect insider threats.	3.02	1.154	38.2	Partly Implemented
1.6	Suspension of the Employees who have committed offence	3.55	1.376	38.8	Implemented
1.7	written warning of the Employees who have committed offence	3.19	1.266	39.7	Partly Implemented
1.8	Verbal warning of the Employees who have committed offence	3.11	1.278	41.1	Partly Implemented
1.9	Immediate arrest of the Employees who have committed offence	3.06	1.351	44.2	Partly Implemented
Mean		3.22	1.245	38.7	Partly Implemented

***Source*:** Primary Data 2015

The table above shows that some of deterrence measures ranked top measures being implemented like Immediate arrest as disciplinary measure if an Institutional staff breach the IS security with coefficient of variation 44.2 percent (mean 3.06), Verbal warning disciplinary measure if an Institutional staff breach the IS security with coefficient of variation 41.1 percent (mean=3.11) while Procedures with regard to outsourcing any institutional Information Systems service or activities with Coefficient of variation 34.9 percent (mean=3.18) are not implemented.

Table 4: Security training and awareness

A1	*Security training and awareness*	*Mean*	*Std. Deviation*	*coefficient of variation*	*Interpretation*
1.1	Staff receiving regular updates on Institutional Information Systems' policies.	3.08	1.009	32.8	Partly Implemented
1.2	Procedures related to asset classification	3.15	1.131	35.9	Partly Implemented
1.3	Procedure for owner accountability to ensure appropriate protection is maintained for each Institutional IS asset.	3.19	1.154	36.2	Partly Implemented
1.4	Updating the staff regularly on the various threats that could harm and adversely affect critical operations of the Institution	3.28	1.201	36.6	Partly Implemented
1.5	Staffs aware of their responsibilities with regard to protecting the Institutional Information Systems' security.	3.17	1.299	41.0	Partly Implemented
Mean		3.17	1.159	36.5	Partly Implemented

Source: Primary Data 2015

It was also discovered in the table above 4.7 that one of the mitigation measures being used by institution is that regular updates of Staff at various levels on Institutional Information Systems' policies with coefficient of variation of 32.8 percent (mean=3.08) these regular trainings training can increase users' ability to interact with software programs but as far as Staffs being aware of their responsibilities with regard to protecting the Institutional Information Systems' security and regularly trained to report any security breach incidences with coefficient of variation of 41.0 percent (mean=3.17) was ranked among the last measures being implemented.

Table 5: Time pressure and Workload

	Time pressure and Workload	*Mean*	*Std. Deviation*	*coefficient of variation*	*Interpretation*
1.1	Employees not feel pressure to do more in their job	3.18	1.015	31.9	Some times
1.2	Institutional data security requirements not making staff members' job harder	3.32	1.14	34.3	Some times
1.3	Institutional bosses' abrupt assignments not usually needed in short time	3.04	1.107	36.4	Some times
1.4	Employees not taking work out of office to be accomplished.	3.1	1.194	38.5	Some times
1.5	Heavy work load not ma king employees make errors.	2.72	1.275	46.9	Some times
Mean		3.07	1.15	37.60	Some times

In terms of finding out if employees have a lot of pressure and workload, employees accepted that Heavy work load does make employees make errors with coefficient of variation of 46.9 percent (Mean 2.72) and Employees do take work out of office to be accomplished with coefficient of variation of 38.5 percent (mean=3.1) which means in order to mitigate human insider threats institutions should not allow Employees to take work out of office to be accomplished since it can be a risk of moving with work outside and it was discovered that Employees do not feel pressure to do more in their job, even if it means cutting corners in some areas in order to complete other tasks with coefficient of variation of 31.9 percent (mean=3.18).

Table 6: Usability of security tools

	Usability of security tools	*Mean*	*Std. Deviation*	*coefficient of variation*	*Interpretation*
1.1	Institutional employees using firewalls	3.41	1.032	30.3	Agreed
1.2	Employees protecting data files using any access control measures e.g., password.	3.73	1.146	30.7	Agreed
1.3	Employees applying strong passwords as a measure to protect un authorized access to institutional data.	3.78	1.239	32.8	Agreed
1.4	The Institution regularly reviewing access rights given to users	3.39	1.119	33.0	Some times
1.5	Employees changing password regularly on their own	3.42	1.167	34.1	Agreed
1.6	Employees being able to protect devices using any access control measures e.g., password, locks,pincode or biometric measures	3.52	1.345	38.2	Agreed
Mean		3.5	1.175	33.2	Agreed

The table above shows that employees agreed that staff members are able to use security tools for example Institutional employees use firewalls with coefficient of variation of 30.3 percent (mean=3.41) and Employees can protect data files using any access control measures e.g., password with coefficient of variation of 30.7 percent (mean=3.73) but in terms of Employees changing password regularly on their own of coefficient of variation of 34.1 percent (mean=3.42) and Employees protecting devices which store data using any access control measures e.g. biometric measures of coefficient of variation of 38.2 percent (mean=3.52) they ranked among the last measures being used but most of the measures were all in use.

Table 7: Motivation as mitigation measure

	Motivation Measures	***Mean***	***Std. Deviation***	***coefficient of variation***	***Interpretation***
1.1	Employees being appreciated	3.38	1.064	31.5	Some times
1.2	full delegation of power when the immediate boss is out of office	3.65	1.222	33.5	Agree
1.3	Employees being promoted on merit based on the set procedures	3.52	1.195	33.9	Agree
1.4	Employees being recognized for the commitment to the Institution	3.29	1.144	34.8	Some times
1.5	Employees being rewarded for the good work done in monetary terms	3.13	1.344	42.9	Some times
Mean		3.39	1.194	35.3	Some times

The table above in general shows that sometimes employees are motivated. For example the results shows that Employees are appreciated for the good work done even when it’s not monetary with coefficient of variation of 31.5percent (mean=3.38) which motivates employees and feel part of the organization but in terms of Employees being rewarded for the good work done in monetary terms was ranked last with coefficient of variation of 42.9percent (mean=3.13) which again can de motivate the employees.

Table 8: Technological mitigation measures

A1	***Technological measures***	***Mean***	***Std. Deviation***	***coefficient of variation***	***Interpretation***
1.	Use of clean-up software	3.55	1.04	29.3	Implemented
2.	Use of Anti-Virus software	3.67	1.079	29.4	Implemented
3.	Use of Security guards	3.76	1.156	30.7	Implemented
4.	User authentications being required before accessing the Institutional data	3.55	1.186	33.4	Implemented
5.	Proper management of Disposing of sensitive media.	3.24	1.096	33.8	Partly Implemented
6.	Using Rollback software to keep track of any changes made to the computers	3.4	1.155	34.0	Implemented
7.	Backing Up Vital institutional information or records regularly.	3.55	1.222	34.4	Partly Implemented
8.	Server logs being reviewed periodically	3.39	1.18	34.8	Partly Implemented
9.	Using systems recovery	3.46	1.21	35.0	Implemented
10	Servers being placed in a secure location,	3.61	1.276	35.3	Implemented
11.	Keeping properly attributes for each removable media applications in the Institution kept from any unauthorized accesses.	3.48	1.243	35.7	Implemented
12.	User entrance log to record and monitor user logs regularly analyzed.	3.21	1.188	37.0	Partly Implemented
13.	Locking of devices to improve the security of hardware equipment	3.42	1.394	40.8	Implemented
14.	Intrusion detection software and host auditing software being installed	3.1	1.269	40.9	Partly Implemented
15.	Implementing fraud detection measures	3.03	1.255	41.4	Partly Implemented
16.	Using event logging software	3.13	1.313	41.9	Partly Implemented
17.	Digital signatures being used	2.88	1.262	43.8	Partly Implemented
18.	Use of biometric system	2.89	1.558	53.9	Partly Implemented
Mean		3.35	1.227	37.0	Partly Implemented

Source: Primary Data 2015

From the table 4.13 above clearly showed that majority of the Technological measures were partly implemented and the following technical mitigation measures were in use in Institutions: Clean-up software to erase files or settings left behind by a user of coefficient of variation of 29.3percent (mean=3.55), Anti-Virus software to detect and remove any spyware threats of coefficient of variation of 29.4 percent (mean=3.67), Security guards to monitor people entering and leaving the Institutional buildings and sites of coefficient of variation of 30.7 percent (mean=3.76) and User authentications are required before accessing the Institutional data of coefficient of variation 33.4 percent (mean=3.55) were ranked among the top four technical mitigation measures in use while Use of biometric system to restrict access to sensitive places with coefficient of variation 53.9 percent (mean=2.89), Digital signatures are used to assure the authenticity of any electronic documents sent via the Institutional network with coefficient of variation 43.8 percent (mean=2.88) and Event logging software to ensure the Institutional computer security records are stored in sufficient detail for an appropriate period of time of coefficient of variation 41.9 percent (mean=3.13) were ranked among the last measures being implement.

4. Conclusion

The study found out that the following were top most Unintentional human insider threats Sharing of secondary storage devices like flash discs, CD, Hard disks of coefficient of variation of 30.58percent (mean=3.8), Losing of Secondary storage devices like flash disks, CD, Hard disk, floppy of coefficient of variation of 35.10 percent (mean=3) and Working on a mobile device e.g. Laptop while travelling, Leaving computers unattended to while the following were identified as the current unintentional human insider threats mitigation measures ;Technological Measures, Deterrence Measures, Time pressure and Workload, Security training and awareness Measures, Usability of security tools Measures and Motivation Measures which were the measure currently in use in mitigating human insider threats and majority were partly implemented. Based on the above findings, the author recommend further investigation on the other unintentional mitigation measure which can be used in mitigating other insider threats on institutional data security for example hackers and none human threats to information security such natural disasters and systems failures.

5. Acknowledgements

This work could not have been possible without the financial assistance and moral support given by the Staff development scheme of Kampala International University more especially, the Chairman Board of Trustees Mr. Hassan Basajjabalaba The Doctoral committee members who inspired for continuous encouragement of this work despite the odds, and above all read through the work paragraph by paragraph and directing till the end. You are real mentors. Finally the authors would like to thank the Universities 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.

6. Reference

1. Baskerville R. Designing Information Systems Security. New York, NY: John Wiley Information Series. 1988.
2. Blumstein A. Introduction. In A. Blumstein, J. Cohen and D. Nagin (Eds.), Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates. Washington, DC: National Academy of Sciences. 1978.
3. Bologna J. Handbook of Corporate Fraud. Boston, MA: Butterworth-Heinemann. 1993.
4. Brussin D. Firewall and proxy servers. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc. 2002.
5. Burcu bulgurcu, Hasan Cavusoglu, Izak Benbasat. Information security policy compliance: an Empirical study of rationality-based beliefs And information security awareness; MIS Quarterly. 2010; 34(3):523-548.
6. Chokhani S. Public Key Infrastructures and Certificate Authorities. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook. 2002.
7. D'Arcy J, Hovav A, Galletta DF. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research. 2009; 20(1):79-98.
8. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quartely. 1989; 13(3):319-340.
9. Einwechter N. Preventing and detecting insider attacks using IDS. 2002. Online document at: http://online.securityfocus.com/infocus/1558.
10. Gillham B. Developing a questionnaire. The pros and Cons of Questionaires New York. 2000.
11. Haugen S, Selin JR. Identifying and controlling computer crime and employee fraud. Industrial Management & Data Systems. 1999; 99(8):340-344.
12. Kankanhalli A, Teo H, Tan BCY, Wei K. An integrative study of information systems security effectiveness. International Journal of Information Management. 2003; 23:139-154.
13. Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information security: management's effect on culture and policy. Information Management & Computer Security. 2006; 14(1):24-36.
14. Kolkowska E, Dhillon G. Organizational power and information security rule compliance. Computers & Security. 2012.
15. Lilly JR, Cullen FT, Ball RA. Criminological Theory: Context and Consequences. Thousand Oaks: Sage Publications. 2002.
16. Loch KD, Carr HH, Warkentin ME. Threats to Information Systems: Today's. 1992.
17. Nelson RR, Cheney PH. Training end users: Exploratory study. MIS Quarterly. 1987; 11(4):547-559.
18. NRC National Research Council―For the Record: Protecting Electronic Health Information. 1997.
19. Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: An action research study. MIS Quarterly. 2010; 34(4): 757-778.
20. Reality Yesterday's Understanding, MIS Quarterly. 16(2):173-186.
21. Russell Miller and Merritt Maxim Dealing with insider threats to cyber-security. 2015
22. Saltzer JH, Schroeder MD. The protection of information in computer systems. Proceedings of the IEEE. 1975; 63(1).
23. Spurling P. Promoting security awareness and commitment. Information Management and Computer Security. 1995; 3(2):20-26.

24. Stanton MS, Stam KR, Guzman I, Caldera C. Examining the linkage between organizational commitment and information security. Paper presented at the Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC. 2003.
25. Straub DW, Nance WD. Discovering and disciplining computer abuse in organization. MIS Quarterly. 1990; 14(1):45-60.
26. Taylor S, Todd PA. Understanding information technology usage: A test of competing models. Information Systems Research. 1995b; 6(2):144-176.
27. Thompson ME, von Solms B. Information security awareness: educating our users effectively. Information Management & Computer Security. 1998; 6(4):167-173.
28. Whitman ME, Mattord HJ. Designing and Teaching Information Security Curriculum, Proceedings of the Info Sec CD Conference, M.E. Whitman (ed.), Kennesaw, GA: ACM. 2004, 1-7.
29. Yayla, ali alper. Controlling insider threats with information security policies. 2010.
30. Yerkes RM, Dodson JD. The relation of strength of stimulus to rapidity of habit-formation. Journal of Comparative Neurology and Psychology. 1908; 18:459-482.