[Mbabazi, 3(5): May2016]
DOI- 10.5281/zenodo.51579

ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ASSESSING INTENTIONAL HUMAN INSIDER THREAT MITIGATION IN UGANDAN UNIVERSITIES

Businge Phelix Mbabazi[*1], Dr. Jehopio Peter[2] and Dr. JWF Muwanga–Zake[3]

[*1]Lecturer Information systems School of Computing and Information Technology, Kampala International University
[2]Senior Lecturer Kampala International University School of Computing and Information Technology
[3]Senior Lecturer Kampala International University School of Computing and Information Technology

ABSTRACT

The purpose of this research paper was to assess the various Intentional threats and the current unintentional human insider threats used in the universities in Uganda. The data was collected using survey method. Sampling from ICT Staff members and heads of Departments in charge of handling institutional data. The questionnaires were distributed to 212 respondents purposively selected respondents from different Nine (9) Universities in Uganda. Reliability and validity tests of the instrument was carried out and were found to be above the recommended values and Descriptive statistics and coefficient of Variation were used to analyze these constructs.

The study found out that Using of secondary storage devices like flash discs, CD, Hard disks and Sharing of secondary storage devices like flash discs, CD, Hard disks, and Working on a mobile device e.g. laptop while travelling, Using of personally owned mobile devices were top threats and the following measures were assessed Technological measures, Deterrence measures were partly implemented , Integration and commitment and Background Information Check of Users were sometimes implemented .

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

Keywords- Insider threats, Intentional Human Insider threats, Mitigation Measures, Universities

1. INTRODUCTION

1.1 Human Insider Threats

Insider attack is "the intentional misuse of computer systems by users who are authorized to access those systems and networks." (Schultz & Shumway, 2001).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) 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

Based on the findings, Ponemon, (2012) recommends that organizations 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), 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.

ISSN 2348 – 8034
Impact Factor- 3.155

1.4 Information Security in the Workplace

According to Yayla & Alper (2010) 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).

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). Although reasons for user errors are numerous, simple lack of awareness of the importance of information security is an obvious factor.

1.5 Intentional human Insider Threats to Institutional Data Security

Schultz and Shumway (2001) defined insider attack as "the intentional misuse of computer systems by users who are authorized to access those systems and networks". Parallel to this definition, we consider computer abuse and fraud as the most common intentional insider threats to information security. Computer abuse is the "unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals" (Straub and Nance, 1990). Violations against hardware, programs, data and computer services are some of the possible computer abusing cases (Straub and Nance, 1990). On the other hand, reasons behind computer fraud cover a wide range from inadequate rewards and management control to lax enforcement of disciplinary rules (Bologna, 1993).

Deterrence is considered as one of the initial steps in preventing computer abuse and fraud. Effective deterrence requires organizations to consider the social psychology of fraud perpetrators and the control environment of the firm by utilizing mechanisms such as employee education, proactive fraud policies, use of analytical reviews, surprise audits, and adequate reporting programs (Bologna, 1993). Considering these point of views, in this section, we address computer fraud and abuse using three mechanisms: Integration and commitment of the employees to the organization, deterrence measures, and technology-based controls.

Integration and Commitment

Integration and commitment. Integration (social or external bond) is the extent to which people are involved in and attached to conventional groups and institutions (Lilly et al., 2002). Commitment, on the other hand, is personal attachment to conventional roles, groups and institutions (Lilly et al., 2002). Parallel to this, Stanton et al. (2003) investigated the relation between organizational commitment and information security and reported that individuals with high organizational commitment are less likely to have behaviors that may put their company at risk.
Some researchers have found out that lack of management support has been singled out as a common reason for the weak implementation of information security policies in organization (Knapp et al. 2006; Kolkowska & Dhillon 2012).
Deterrence Measures

Deterrent factors are considered passive administrative countermeasures; hence, their effectiveness depends completely on individuals (Straub and Welke, 1998). Awareness programs and policies/guidelines that specify proper use of computer systems are two of the most effective deterrence measures (Straub & Nance, 1990). Studies in the information systems (IS) literature found empirical support in favor of the effectiveness of deterrence measures (Kankanhalli et al., 2003; Lee et al., 2004). However, in order to be effective, deterrence measures should communicate disciplinary actions that will be exercised when perpetrators are identified (Blumstein, 1978). For instance, D'Arcy et al. (2009) reported that perceived certainty and perceived severity of sanctions have negative effect on IS misuse intentions.

INSA (2013) argues 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 (Straub, 1986; Baskerville, 1988). The aim of preventive control is towards reducing possible threats (Baskerville, 1988), 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

ISSN 2348 – 8034
Impact Factor- 3.155

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) 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). Sandhu (2002) 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). 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). Some of the more advanced computer-based controls that can be implemented are public key infrastructures, certificate authorities, and vulnerability assessment (Chokhani, 2002).

Background User Check

A background check or background investigation is the process of looking up and compiling criminal records, commercial records and financial records of an individual or an organization. Background checks are often requested by employers on job candidates for employment screening, especially on candidates seeking a position that requires high security or a position of trust, such as in a school, hospital, financial institution, airport, and government. These checks are often used by employers as a means of judging a job candidate's past mistakes, character, and fitness, and to identify potential hiring risks for safety and security reasons. Some employers may conduct criminal background checks on job applicants voluntarily to identify those who may commit criminal acts in the workplace in order to minimize loss and legal liability of negligent hiring that could result from such acts (Bushway, 1998).

Apart from employees past records, the institution should have continuous background user information checks while on job and after he has left the job, for example even when he/she has left the organization, the former insider can leave a loophole in the system or still access the institution information illegally.

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=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.

2.1 Population and Sample size

Table 1: Population and Sample size

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

ISSN 2348 – 8034
Impact Factor- 3.155

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), 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: Intentional Human Insider threats

A1	*Human Insider Threat*	*Mean*	*Std. Deviation*	*coefficient of variation*	*Interpretation*
1.	Using of secondary storage devices like flash discs, CD, Hard disks.	3.9	1.162	29.79	Frequent
2.	Sharing of secondary storage devices like flash discs, CD, Hard disks.	3.8	1.162	30.58	Frequent
3.	Working on a mobile device e.g. laptop while traveling	3.1	1.161	37.45	Sometimes Frequent
4.	Deleting information on their computer when no longer necessary.	2.5	1.024	40.96	Sometimes Frequent
	Using of personally owned mobile devices to do office work	3	1.236	41.20	Sometimes Frequent
	Failing to have automatic lock of the screen savers	2.9	1.275	43.97	Sometimes Frequent
	Disclosing Institutional information to others, e.g. email message sent to wrong address or an information leak through peer-to-peer file sharing	1.9	0.866	45.58	Not Frequent
	Insiders transmitting employees' information to outsiders for gain.	1.8	0.926	51.44	Not Frequent
	Connecting computers to the Internet through an insecure wireless network	1.9	0.999	52.58	Not Frequent
	Reusing the same password and username on different logins	2.2	1.157	52.59	Not Frequent
	Sharing of passwords with other staff members	2.3	1.246	54.17	Not Frequent
Mean		2.7	1.1107	43.667	Sometimes Frequent

According to the data obtained from Institutional Employees above from the field the following risky intentional human insider behaviours were ranked among the top frequently happening: Using of secondary storage devices like flash discs, CD, Hard disks

ISSN 2348 – 8034
Impact Factor- 3.155

of coefficient of variation of 29.79 percent (mean=3.9) and Sharing of secondary storage devices like flash discs, CD, Hard disks of coefficient of variation of 30.58percent(mean=3.8) , and Working on a mobile device e.g. laptop while travelling, Leaving computers unattended to, Deleting information on their computer when no longer necessary, Using of personally owned mobile devices to do office work, Failing to have automatic lock of the screen savers were among the top ten behaviours practiced by institutional employees in institutions which are one of the source of leakage of Institutional data either intentionally or unintentionally.

3.2 Current Intentional Human Insider Threats Mitigation Measures

Table 3: Background Information Check of Users

	Background Information Check of Users	*Mean*	*Std. Deviation*	*coefficient of variation*	*Interpretation*
1.1	Checking out the applicant's character references /academic qualifications/ personal identify.	3.35	1.014	30.3	Sometimes carried out
1.2	Performing more rigorous background checks when the perceived security risk is greater?	3.26	1.054	32.3	Sometimes carried out
1.3	Performing more rigorous background checks on people who will be accessing information.	3.17	1.066	33.6	Sometimes carried out
1.4	Background checks complying with all relevant labor and employment legislation and personal data protection legislation.	3.06	1.072	35.0	Sometimes carried out
1.5	Background checks procedures defining why background checks should be performed.	3.03	1.099	36.3	Sometimes carried out
1.6	Background checks of contractors/ third-party users	2.95	1.123	38.1	Sometimes carried out
1.7	Background checks of candidates for employment	2.8	1.228	43.9	Sometimes carried out
Mean		3.09	**1.094**	**35.6**	**Sometimes carried out**

Source: Primary Data 2015

The table above clearly indicates that institutions apply some mitigation measures of human insiders and they do check out the applicant's character references /academic qualifications/ personal identify with coefficient of variation of 30.3percent(mean =3.35) but they rarely check the backgrounds of candidates for employment before you allow them to access your organization's information with coefficient of variation 43.9percent (mean=2.8) but the Institutional Employees ranked the measure of checking the backgrounds of candidates for employment before you allow them to access your organization's information with coefficient of variation 43.9percent(mean=2.8) as the last measure on background checks.

ISSN 2348 – 8034
Impact Factor- 3.155

Table 4: Deterrence mitigation measures

	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 44.2percent(mean 3.06), Verbal warning disciplinary measure if an Institutional staff breach the IS security with coefficient of variation 41.1percent(mean=3.11)while Procedures with regard to outsourcing any institutional Information Systems service or activities with Coefficient of variation 34.9percent(mean=3.18) are not implemented.

Table5: Integration and commitment

	Integration and commitment	Mean	Std. Deviation	coefficient of variation	Interpretation
1.1	Employees IT security skills helping them to do their jobs better.	3.76	1.09	29.0	Agree
1.2	Employees knowing how Institutional data security affects their job.	3.56	1.054	29.6	Agree

ISSN 2348 – 8034
Impact Factor- 3.155

1.3	Positive commitments from the top management on Security of Information	3.5	1.099	31.4	Some times
1.4	Management regularly advising employees to think about protecting institutional data every day as part of their job.	3.08	1.357	44.1	Some times
1.5	Employees being concerned to know about the security risks of using IT assets	2.88	1.433	49.8	Some times
Mean		**3.36**	**1.207**	**36.8**	**Some times**

Employees also cited out that Employees IT security skills help them to do their jobs better with coefficient of variation of 29.0 percent (mean=3.76) and they know how Institutional data security affects their job with coefficient of variation of 29.6 percent (mean=3.56) which shows that there is commitments by institutional employees and feel part of the institutions.

Table6. : Technological mitigation measure

	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
	Server logs being reviewed periodically	3.39	1.18	34.8	Partly Implemented
	Using systems recovery	3.46	1.21	35.0	Implemented
	Servers being placed in a secure location,	3.61	1.276	35.3	Implemented
	Keeping properly attributes for each removable media applications in the Institution kept from any unauthorized accesses.	3.48	1.243	35.7	Implemented
	User entrance log to record and monitor user logs regularly analyzed.	3.21	1.188	37.0	Partly Implemented
	Locking of devices to improve the	3.42	1.394	40.8	Implemented

ISSN 2348 – 8034
Impact Factor- 3.155

	security of hardware equipment				
	Intrusion detection software and host auditing software being installed	3.1	1.269	40.9	Partly Implemented
	Implementing fraud detection measures	3.03	1.255	41.4	Partly Implemented
	Using event logging software	3.13	1.313	41.9	Partly Implemented
	Digital signatures being used	2.88	1.262	43.8	Partly Implemented
	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 29.4percent(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 33.4percent(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 53.9percent(mean=2.89), Digital signatures are used to assure the authenticity of any electronic documents sent via the Institutional network with coefficient of variation 43.8percent(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. CONCLUSIONS

The study found out that the following were Using of secondary storage devices like flash discs, CD, Hard disks , Sharing of secondary storage devices like flash discs, CD, Hard disks and Working on a mobile device e.g. Laptop while travelling, Using of personally owned mobile devices to do office work, were top ranked Intentional human insider threats and the following measures were identified Technological Measures, Background Information Check of Users, Deterrence Measures and Integration and commitment as the current measure in use in mitigating intentional human insider threats and majority were partly implemented.

Based on the above findings, the author recommend further investigation on the other intentional human insider threats 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.

ISSN 2348 – 8034
Impact Factor- 3.155

REFERENCES

1) *Ajzen, I. "The Theory of Planned Behavior," Organizational Behavior and Human Decision Processes, Vol. 50, No. 2: 179-211, 1991.*

2) *Baskerville, R. (1988). Designing Information Systems Security. New York, NY: John Wiley Information Series.*

3) *Blumstein, A. (1978). 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*

4) *Bologna, J. (1993). Handbook of Corporate Fraud. Boston, MA: Butterworth-Heinemann.*

5) *Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2010). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18, 151-164.*

6) *Brussin, D. (2002). Firewall and proxy servers. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc.*

7) *Burcu bulgurcu ,Hasan Cavusoglu and Izak Benbasat (2010) information security policy compliance: an Empirical study of rationality-based beliefs And information security awareness; MIS Quarterly Vol. 34 No. 3 pp. 523-548/September 2010*

8) *Chokhani, S. (2002). Public Key Infrastructures and Certificate Authorities. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook.*

9) *D'Arcy J, Hovav A & Galletta DF (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1): 79–98.*

10) *Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quartely,13 (3), 319-340.*

11) *Einwechter, N. (2002). Preventing and detecting insider attacks using IDS, Online document at: http://online.securityfocus.com/infocus/1558.*

12) *Gillham, B. (2000). Developing a questionnaire. The pros and Cons of Questionaires New York:*

13) *Haugen, S. and Selin, J.R. (1999). Identifying and controlling computer crime and employee fraud. Industrial Management & Data Systems, 99(8), 340-344.*

14) *INSA, A preliminary examination of insider threat programs in the U.S. private sector,*

15) *Intelligence and National Security Alliance, Cyber Council: Insider Threat Task Force, 2013*

16) *Kankanhalli, A., Teo, H., Tan, B.C.Y. and Wei, K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23, 139-154.*

17) *Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security , 14(1), 24-36.*

18) *Kolkowska, E., & Dhillon, G. (2012). Organizational power and information security rule compliance. Computers & Security.*

19) *Lilly, J.R., Cullen, F.T. and Ball, R.A. (2002). Criminological Theory: Context and Consequences. Thousand Oaks: Sage Publications.*

20) *Loch, K.D., Carr, H.H., and Warkentin, M.E. 1992. "Threats to Information Systems: Today's*

21) *Nelson, R.R. and Cheney, P.H. (1987). Training end users: Exploratory study. MIS Quarterly, 11(4), 547-559.*

22) *NRC National Research Council (1997) —For the Record: Protecting Electronic Health Information*

ISSN 2348 – 8034
Impact Factor- 3.155

23) Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778.

24) R. Richardson, "CSI computer crime&security survey," http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf (last viewed May 2013), 2008.

25) Reality, Yesterday Understands," MIS Quarterly (16:2), pp. 173-186.

26) Russell Miller and Merritt Maxim (2015) Dealing with insider threats to cyber-security

27) Saltzer, J.H. and Schroeder, M.D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(1).

28) Spurling, P. (1995). Promoting security awareness and commitment. Information Management and Computer Security, 3(2), 20-26.

29) Stanton, M.S., Stam, K.R., Guzman, I. and Caldera, C. (2003). Examining the linkage between organizational commitment and information security. Paper presented at the Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC.

30) Straub & Welke RJ (1998) Coping With Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly 22(4): 441–469.

31) Straub & Welke RJ (1998) Coping With Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly 22(4): 441–469.

32) Straub, D.W. and Nance, W.D. (1990). Discovering and disciplining computer abuse in organization. MIS Quarterly, 14(1), 45-60.

33) Taylor, S. and Todd, P.A. (1995b). Understanding information technology usage: A test of competing models. Information Systems Research, 6(2), 144-176.

34) Thompson, M.E. and von Solms, B. (1998). Information security awareness: educating our users effectively. Information Management & Computer Security, 6(4), 167-173.

35) 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.

36) Yayla and ali alper(2010) controlling insider threats with information security policies

37) Yerkes, R.M. and Dodson, J.D. (1908). The relation of strength of stimulus to rapidity of habit-formation. Journal of Comparative Neurology and Psychology, 18, 459-482.