International Journal on Advanced Science Engineering Information Technology

Vol.7 (2017) No. 5
ISSN: 2088-5334

Investigation of Attributes that Influence the Insider Trust

Rohayanti Hassan[1*], Iszaida Ismail[1], Shahreen Kasim[2], Muhammad Razib Othman[1], Rohaizan Ramlan[3]

[1]*Department of Software Engineering, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia*
[2]*Soft Computing and Data Mining Centre, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn, Johor, Malaysia*

[3] *Faculty of Technology Management and Business, Universiti Tun Hussein Onn, Johor, Malaysia*
**E-mail: rohayanti@utm.my*

Abstract **— A study of cyber-attack incidents emanating from insiders identifies some characteristic of the malicious user including trust, attack on hardware, software and network, and vulnerabilities of threat. Among the research that has been conducted, insider trust is identified as a critical characteristic where trust of insider is categorized as a major potential to attack system information either high, medium or low risk to access the sensitive document. Trust characteristics is hard to be analyzed due to the different human behaviour. Thus, a survey was conducted that includes hypothesis to support the investigation of insider threat characteristic. To obtain the result of finding prominent insider trust criteria, a regression analysis is used to get the actual value. A survey has been distributed to multiple user roles of three systems namely e-Plantation System (ePS), eCampus System (eCampus) and Human Resources Management System (eHRMS). The outcome of this study demonstrates that skill and experience are two prominent factors that mainly influence the characteristic of insider trust.**

Keywords— Insider **trust; insider threat; insider threat prediction; trust characteristics; insider trust criteria.**

I. INTRODUCTION

Information security is the most pressing challenges confronting all kinds of contemporary organizations. Since data is an important asset for individuals and organizations, mechanisms that protect data from interception, modification and fabrication in such systems have become critical. Besides, a deliberate risk to organization and private security is the disclosure of secure data in transmission and storage [1]. It is important to ensure data confidentiality, integrity and availability are secured and protected. One of the major issues in computer security is the insider threat posed by users of a system. This threat is increasing at an unprecedented rate. According to the 2012 Cyber Security Watch Survey, about 51% of information security incidents and damage was attributed to insider attacks rather than outsider attacks. Insiders pose a high security risk to the system due to their legitimate access, knowledge and trust about the organization and the location of valuable assets [2]. Mostly, a core cause of insider attacks is the attitudes of an insider especially their trust towards the system.

Insider problem is often touted as one of the most serious security problems and issues that are most difficult to deal with [3]. Most commonly response of 'insiders' is that they are internal employees who work for the organization. Even [4] defines the threat as a threat that comes from people who have been granted access to the information system and abusing their rights, thereby violating information system security policy of the organization. Mundie et. al. [5] define insider as a people, employees or former employees, contractors, or business partners who had an authorized access to the network, system, or data organization. Sometimes, they are intentionally exceeded or misused the access which lead to negative impact on the confidentiality, integrity, or availability of information or information systems organization. However, [6] defines an insider as an individual that has been lawfully granted the ability to access one and more module in the IT infrastructure, by interacting with each authentication mechanisms. Meanwhile, the insider threat can be defined as a person who is believed to have the privilege and access the system that potential to do harm to the system and its data.

Nowadays, insider trust becomes more incomprehensible and disconcerting problem. Based on the previous research, although a trust attribute of an insider has been identified, however, empirical research regarding insider behaviour and attribute that influencing their trust in using the system is still in infancy. A few overarching attributes of insider trust show that organizations should take consideration of major impact where insider potential to harm their systems. Table 1 indicates the insider trust attributes that categorizes into

two types which are internal factor and external factor. Internal factor comprises attributes of experience, skill and responsibility which demonstrate a natural processes [7] behavioural of an insider. Internal factor is categorized based on the characteristics of insider itself that more pressing on aspects of personal interest. Other example of internal factors is user action in system, user intention, usability, integrity and confidentiality. While policy and system security was grouped into external factors. External factor is circumstances or situations outside of the insider characteristics. Each external factor can be identified based on outside source [8] and cannot be determined based on insider capabilities such as target attack, operating systems, human safety and others.

Thus, this paper is motivated to investigate and discuss the attributes that influence the degree of insider trust. This paper will be explained more details regarding the method used, statistical measurement and the result respectively in section 2, 3 and 4.

II. MATERIAL AND METHOD

A. Identify Attributes

A depth research has been conducted earlier that eventually highlight there are five attributes are identified as mostly common factors that influence the insider trust. There are experience, skill, policy, security system and responsible as illustrated in Table 1. This study has chosen data leakage as the security threat issue which consist of five components to be analysed, namely computer usage, solving bugs, server and network fine tuning, security policy and system handling as presented in Fig 2.

B. Construct the Hypothesis

Next hypothesis is set up. Table 2 presents the set up hypothesis for each attributes and its respective survey questions.

C. Design A Research Model

Following the preceding discussion, the investigation model or commonly termed as research model is presented in Fig 1. It can be seen that both internal and external factors are combined and are believed has an impact in insider trust and also associate to the occurrence of data leakage. Each of insider attributes are associated to the degree of data leakage exposure via hypothesis statement (H1, H2, H3, H4 and H5).

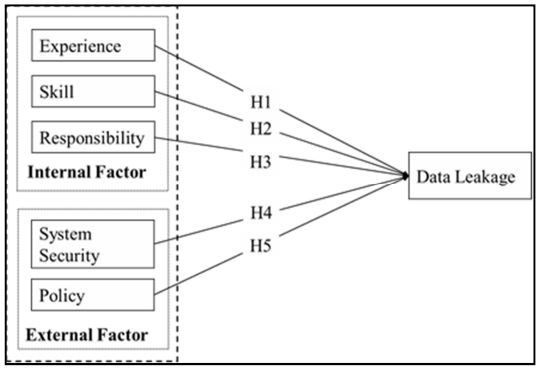

Fig. 1 A Research Model

TABLE I
INSIDER TRUST ATTRIBUTES

Attribute	Description	Research Work
Experience	Experience gained from normal use and experiments; familiarity with sensitive files, project knowledge; collusion easy.	[9]
	Experienced resources and insider abuse the network.	[10]
Skill	The technical expertise dimension focused on the degree of computer or information technology knowledge and skill.	[11]
	The knowledgeable insider will always have the skills to mount an attack that is usually limited to systems.	[12]
Policy	Employees' compliance with organizational rules, guidelines, and requirements laid out in their information systems security policy as a useful mechanism for shaping or influencing the behaviours of their employees.	[13]
	19.9% work in companies that do not enforce their acceptable use policy.	[11]
	Ensuring security policy compliance and security-conscious behaviors are important because it has been found for example that people may ignore or disable security measures.	[14]
Security system	Computer and information security provides protection to users by creating awareness of threats and risks posed by computing on the internet.	[15]
	User awareness and education are critical in mitigating cyber threats such as targeted phishing and would enable individuals and business.	[16]
Responsible	Trusted insiders are responsible for 52% of all security breaches.	[17]
	Organizations with employees who participate in various activities and have increased responsibilities are more likely to develop a security culture and establish a high level of security awareness among their personnel.	[18]

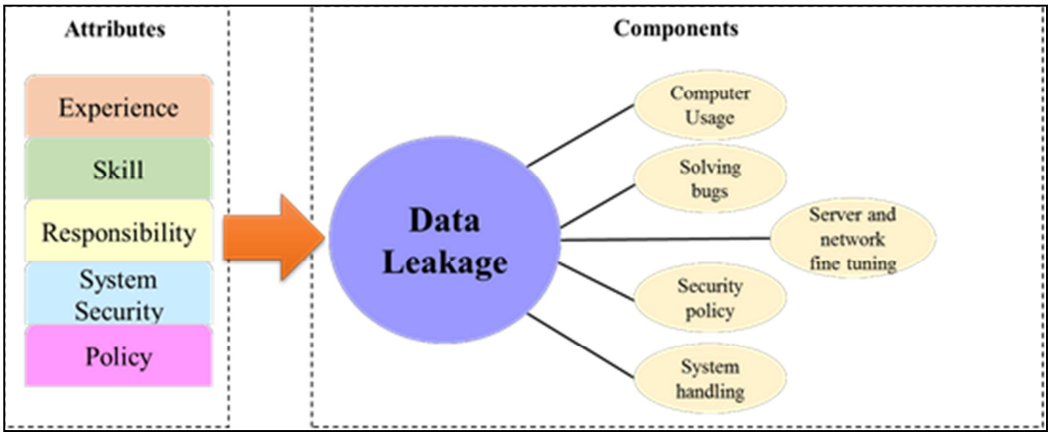

Fig. 2 Trust Component based on skill and experience

TABLE II
HYPHOTESIS MAPPING

Attribute	Questionnaire	Hypothesis
Experience	• Insider that has a good experience on computer usage are positively associated to low expose in data leakage. • Insider with poor experience in handling system are positively associated to low expose in data leakage. • Insider with poor experience in solving error or bug are positively associated to low expose in data leakage. • Insider with good experience on security policy are positively associated to low expose in data leakage. • Insider with good experience on fine tune server and network are positively associated to low expose in data leakage.	**(H1):** An experienced insider is more trusted and will be positively associated to low expose in data leakage.
Skill	• Insider that has high skill on computer usage are positively associated to low expose in data leakage. • Insider with low skill in handling the system are positively associated to low expose in data leakage. • Insider with high skill in solving error or bug are positively associated to low expose in data leakage. • Insider with low skill on security policy are positively associated to low expose in data leakage. • Insider with low skill on fine tuning server and network are positively associated to low expose in data leakage.	**(H2):** A skillful insider is more trusted and will be positively associated to low expose in data leakage.
Responsibility	• Insider with heavy responsibility in computer usage are positively associated to low expose in data leakage. • Insider with less responsibility in handling the system are positively associated to low expose in data leakage. • Insider with heavy responsibility in solving error or bug are positively associated to low expose in data leakage. • Insider with heavy responsibility on security policy are positively associated to low expose in data leakage. • Insider with heavy responsibility on fine tuning server and network are positively associated to low expose in data leakage.	**(H3):** A responsible insider is more trusted and will be positively associated to low expose in data leakage.
Policy	• Insider with high policy awareness in policy of computer usage are positively associated to low expose in data leakage. • Insider with low policy awareness in handling the system are positively associated to low expose in data leakage. • Insider with low policy awareness of solving error or bug are positively associated to low expose in data leakage. • Insider with low policy awareness of security policy are positively associated to low expose in data leakage. • Insider with low policy awareness of fine tune server and	**(H4):** A strict policy makes insider is more trusted and will be positively associated to low expose in data leakage.

Attribute	Questionnaire	Hypothesis
	network are positively associated to low expose in data leakage.	
Security system	• Insider with high concern on computer usage security are positively associated to low expose in data leakage. • Insider with low concern on handling the system security are positively associated to low expose in data leakage. • Insider with high concern in solving error or bug are positively associated to low expose in data leakage. • Insider with high concern on security policy are positively associated to low expose in data leakage. • Insider with high concern on fine tuning server and network are positively associated to low expose in data leakage.	**(H5):** A security system awareness makes insider is more trusted and will be positively associated to low expose in data leakage.

D. Conduct Survey

We have conducted a survey towards a user of a real system which known as e-Plantation System (ePS), eCampus System (eCampus), Human Resources Management System (eHRMS) that include diverse user roles and background. According to [19] survey is one type of research method that comes in many different methods, from door-to-door, telephone, mail, as well as online survey. Thus, questionnaires has been selected in this survey. Questionnaire was distributed to multi roles of user of those three systems. There were 188 completed questionnaires were received which equivalent to 99.5% usable response rate.

Preliminary analyses have reported the analysis of respondent background information such as gender, education level, user role, and age and year involvement as depicted in Fig 3(a) - (e). Fig 3(a) shows that the number of female respondent is greater than the number of male respondent. Besides, a high percentage education level is dominated by the degree holder respondent about 69% while SPM holder respondent is only 1% as represented in Fig 3(b). Meanwhile, Fig 3(c) shows that mostly respondents are system user. Fig 3(d) and 3(e) shows the age of respondent is between 18 and 30 and most of the respondent is less than three years involvement in handling their system respectively.

E. Statistical Measurement

The survey was divided into six section which are, basic information, an experience of insider, a skill of insider, security policy, system security awareness and insider responsibility.

For all question that related to attribute we used five-point Likert style scales ranging from 1 = "Strongly Disagree" through to 3 = "Neither Disagree nor Agree" and 5= "Strongly Agree". The users were selected based on their user roles in the system (i.e. developer, system administrator, system support, and end-user).

Next, all questionnaire that has been completed was extracted in order to get the mean, standard deviation (SD), correlation, regression and hypothesis result. Statistical analysis [20] acknowledges no evidence on non-normality in the distribution of insider threat attribute. Therefore, the present took into account the function of the regression analysis model in order to assess the relationships between the analyzed attributes. The purpose of each data results is required in this study is due to help us to simplify large amounts of data in a sensible way, to shows relationship between attributes, and to correctly specify the relationship between the attributes being used.

The mean or average is used to describe the central tendency of each attribute which are skill, experience, policy, system security, and responsibility. To calculate the mean is add up all the values and divide by the number of values. The formula to calculate the mean is as follows:

$$\text{Mean, } \bar{x} = \frac{\sum x}{n} \quad (1)$$

Where $\sum x$ is the sum of all data value, N is a number of the data item in population, and n is number of data items in samples. Next, a standard deviation is used to measure the dispersion, or how spread out the attribute data are from the mean. The greater the standard deviation, the greater the spread in the attribute data. The standard deviation is a more accurate and detailed estimate of dispersion because an outlier can greatly exaggerate the range. To get the standard deviation, we take the square root of the variance. The formula used for calculated standard deviation is as follows:

$$\text{Standard deviation} = \sqrt{\sum \left(\frac{\mu - \bar{\mu}}{n-1}\right)^2} \quad (2)$$

Where μ stand for each score, $\bar{\mu}$ is mean, n represent the number of value and $\sum$ means sum across the values. The variance measures how much the attribute data are scattered about their mean. The variance is equal to the standard deviation squared. Furthermore, a correlation is used to describe the degree of relationship between each attribute and its component as illustrated in Fig 2. These relationships including each attribute experience, skill, responsibility, system security and policy towards the component of data leakage which are computer usage, bug solving, server and network fine tune, security policy and system handling. Thus, the r symbol was used to stand for the correlation. The formula for the correlation is as follows:

$$r = \frac{N\sum xy - (\sum x)(\sum y)}{\sqrt{[N\sum x^2 - (\sum x)^2][N\sum y^2 - (\sum y)^2]}} \quad (3)$$

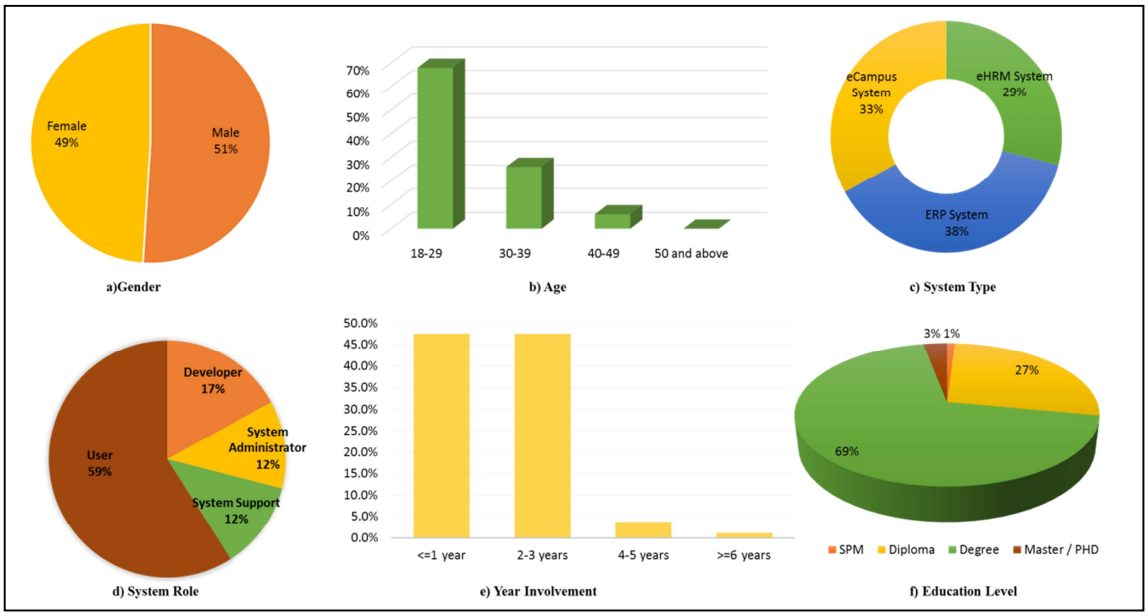

Fig.3 Statistic Analysis of Respondent Background

Where, N is number of pairs of scores, $\sum xy$ is sum of the products, $\sum x$ is sum of x scores, $\sum y$ is sum of y scores, $\sum x2$ is sum of square x and $\sum y2$ is sum of squared y. A linear regression model analysis is implemented in order to measure the significance coefficients. Regression analysis is generated to describe the statistical relationship between attributes and the responses. Then, significance test can be conducted. Firstly the significance level can determined. The common significance level is set with p-value 0.05. If the p-value is less than 0.05 that indicates to reject the null hypothesis. In other words, an attributes that has p-value greater than 0.05 is likely to be a meaningful addition because changes in the attributes value are related to changes in the components attributes. While, regression coefficients represent the mean change in the components variable for one unit of change in the attributes holding other attributes in the model constant. This statistical control that regression provides is important because it isolates the role of one attributes from others in the study. All the subsequent results of the study were analyzed using a regression model, as shown in Table 3 that highlights all the path coefficients representing the standard beta weight.

III. RESULT AND DISCUSSION

Fig 4(a), 4(b) and 4(c) present hypothesis result for ePS system, eCampus System and eHRMS system respectively. Hypothesis will be rejected whenever the path coefficient value is negative. As shown in Fig 4(a) and 4(b), only H5 is rejected, while in Fig 4(c) two hypothesis are rejected which are H2 and H3. Next, to identify the accepted hypothesis, p-value of each hypothesis is then calculated. Furthermore, Table 3 shows the overall finding of the hypothesis based on the regression analysis that has been conducted. These finding also include the path coefficient and p-value for each system.

The result analysis strongly supported the hypothesis when p-value is less than 0.05 and show it is very significant. Thus, as states in result, for ePS system, H1, H2, and H4 are accepted. For eCampus system, accepted hypothesis is H1, H3 and H4. However, for eHRMS, results show that H2 and H3 are accepted. Table 4 shows the summarized results of the hypothesis.

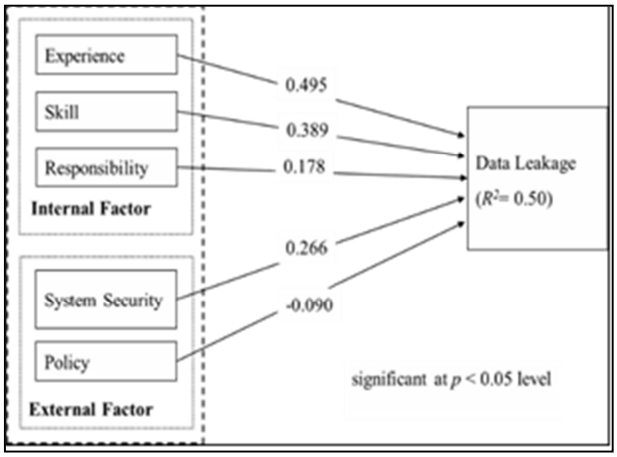

Fig.4(a) Hypothesis result for ePS System

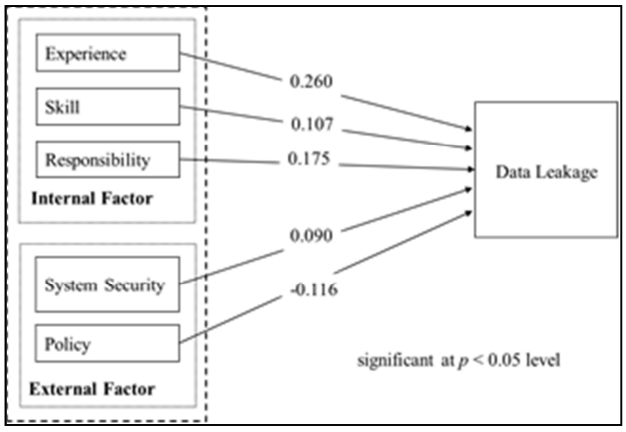

Fig.4(b) Hypothesis result for eCampus System

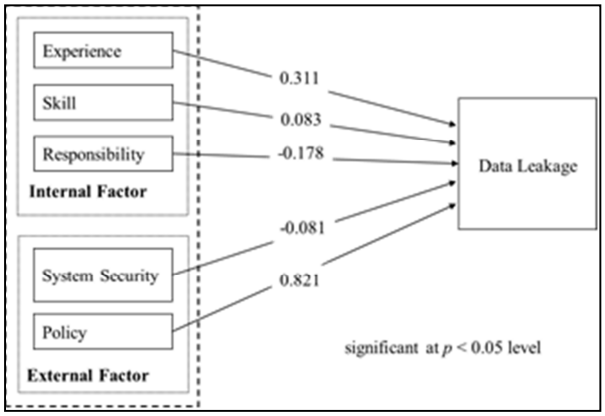

Fig.4(c) Hypothesis result for eHRMS

The accepted hypothesis are H1, H2 and H4 for every system while the hypothesis satisfy the path coefficient and p-value. Besides, these result shows the correlation between the variable is very strong and associated to low expose in data leakage. In addition, some researcher such [21] also support that insider skill and experience increase when the attribute of trust, understanding and knowledge regarding the system structure is lack. Insider with high skill also can produces unexpected results which can be reflected in the performance of the system. The exact cause based upon the result of our study cannot be determined, but it is conceivable those insiders that has less skill in computer usage, but has high knowledge in the system domain are able to control the system, thus able to react to security threats.

TABLE III
Overall Findings from Regression Analysis

Tested Path	Path Coefficient (β)			p- value		
	ePS	eCampus	eHRMS	ePS	eCampus	eHRMS
H1	0.495	0.260	0.311	0.000	0.0012	0.081
H2	0.389	0.107	0.083	0.000	0.0621	0.009
H3	0.178	0.175	-0.178	0.169	-0.288	0.064
H4	0.266	0.090	-0.081	0.000	0.002	0.104
H5	-0.090	-0.116	0.821	0.030	0.000	-0.008

TABLE IV
ACCEPTANCE RESULT

Hypothesis	Significant?	Supported?
H1: An experienced insider is more trusted and will be positively associated to low expose in data leakage.	Yes	Yes
H2: A skilful insider is more trusted and will be positively associated to low expose in data leakage.	Yes	Yes
H3: A strict policy makes insider is more trusted and will be positively associated to low expose in data leakage.	No	No
H4: A security system awareness makes insider is more trusted and will be positively associated to low expose in data leakage.	Yes	No
H5: A responsible insider is more trusted and will be positively associated to low expose in data leakage.	Yes	No

IV. CONCLUSIONS

Due to the high security risk to the system information nowadays that exposed by the insider threat, the study has come out by identified a critical trust characteristic of insiders. Insider are describes as a major potential attacked the system information in which the exploration of the insider trust attribute in enterprise system management are conducted. A survey towards insider characteristics which is knowledge, skill, responsibility, system security and policy are implemented among. The empirical results and analysis show that the objective was achieved. The evidence clearly suggests that the skill and experience of an insider contribute to prominent and critical attributes that lead to main factors of insider attacked.

ACKNOWLEDGMENT

This work is supported by MyMaster Scholarship of the Ministry of Education Malaysia, RMC UTM, G-Heart scheme under the Gates Scholars Foundation and GUP grant, with Vot No: 4C097.

REFERENCES

[1] S. V. Gaikwad, S. Chougule and S. Charhate,"Detection and Prevention of Sensitive Data From Data Leak Using Shingling and Rabin Filter," International Journal on Advanced Science, Engineering and Information Technology, vol. 6, no. 5, pp. 663-667, 2016.

[2] C. Colwill, “Human factors in information security: The insider threat - Who can you trust these days?” Inf. Secur. Tech. Rep. vol.14,pp.186–196, 2009.

[3] M. Bishop, S. Engle, D. A. Frincke, C. Gates, F. L. Greitzer, S. Peisert, and S. Whalen, “A Risk Management Approach to the “ Insider,” pp. 1–24.

[4] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, (2005). The insider threat to information systems and the effectiveness of ISO17799. Comput. Secur., vol. 24, no. 6, pp. 472–484.

[5] D. A. Mundie, S.Perl, & C. L. Huth, “Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions” Work. Socio-Technical Asp. Secur. Trust. STAST, pp. 26–36, 2013.

[6] G. B. Magklaras, and S. M. Furnell, “A preliminary model of end user sophistication for insider threat prediction in IT systems”, Computers and Security, vol.24, no.5, pp.371–380, 2005.

[7] M. Jouini, L. B. A. Rabai, & A. Ben. Aissa, (2014). Classification of security threats in information systems. Procedia Comput. Sci. vol.32, pp. 489–496.

[8] S. Furnell,”Enemies within: The problem of insider attacks” Comput. Fraud Secure, pp. 6–11, 2004.

[9] P. G. Neumann, (2010). Combatting insider threats. Adv. Inf. Secur., 2010.

[10] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, “Insiders Behaving Badly : Addressing Bad Actors and Their Actions,” vol. 5, no. 1, pp. 169–179, 2010.

[11] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, “Analysis of end user security behaviors”. Comput. Secur., vol. 24, no. 2, pp. 124–133, 2005.

[12] G. B. Magklaras and S. M. Furnell, “A Preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems”, 2010

[13] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” Comput. Secur., vol. 31, no. 1, pp. 83–95, 2012.

[14] M. Workman, “A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions”, Inf. Organ, vol.19, pp.218–232,2009.

[15] S.Mubarak, and J. Slay, “Protecting clients from insider attacks on trust accounts”, Information Security Technical Report, vol.14, no.4, pp. 202–212, 2009.

[16] K. K. R. Choo, “The cyber threat landscape: Challenges and future research directions”, Comput. Secure, vol. 30, pp.719–731, 2011.

[17] Q. Yaseen and B. Panda, “Insider threat mitigation: Preventing unauthorized knowledge acquisition,” Int. J. Inf. Secur., vol. 11, no. 4, pp. 269–280, 2012.

[18] M. Karyda, E. Kiountouzis, & S.Kokolakis, “Information systems security policies: a contextual perspective”, Comput. Secur. Vol.24, pp.246–260, 2005.

[19] P. I. Santosa,"Measuring User Experience During a Web-based Survey: A Case of Back-to-Back Online Surveys," International Journal on Advanced Science, Engineering and Information Technology, vol. 6, no. 3, pp. 339-344, 2016.

[20] G. Krstić, “Asthma prevalence associated with geographical latitude and regional insolation in the United States of America and Australia”, PLoS One 6.

[21] C. Posey, R. J. Bennett, and T. L. Roberts, “Understanding the mindset of the abusive insider: An examination of insiders’ causal reasoning following internal security changes”, Comput. Secur., vol. 30, no. 6–7, pp. 486–497.