Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTERNAL THREATS ON INFORMATION SYSTEM SECURITY IN IRAQ HOSPITALS

[1]MOHAMMED H. SHABAN, [2] NOR HIDAYATI ZAKARIA
[1,2]Faculty of Computing, Universiti Teknologi Malaysia, 81310, Skudai, Johor, Malaysia
E-mail: [1] Mohammed.hssh@gmail.com, [2] hidayati@utm.my

ABSTRACT

Managing security of medical information is currently experiencing significant challenges. "People issue" and "organization issue" have been identified as the most important challenges in this field. An organization internal threats have been considered as a serious danger which arise when the insiders commit fraud or steal sensitive information for personal monetary gain or to seek revenge. The organization is vulnerable to such attacks when the employees are compromising the organization's security to get jobs done. On top of them, human resource managing is a daunting task especially when the organization has consultants, management personnel, partners, and other types of employees as well as a complex operational infrastructure. Insider attacks incur unfathomable losses to the organization through loss of revenue, reputation, intellectual property, and even human life. As such, it is vital that the information system's security management is secured and maintained regardless of the multitude of human factors involved. This paper analyze the internal organizational human factors that could cause an information security breach in Iraq hospitals. We collected 301 samples from internal officers of 5 major publicly held hospitals in Iraq to examine the malicious human factors (MHF) that threatening the patients' personal information and measure the (MHF) to identify the most influential factors.

Keywords: *Health Care Information System, Information Security, Insider Threats, Malicious Human Factors*

1. INTRODUCTION

Information system security management has become a priority for every organization that wants to succeed because of the advent of the digital age. It has driven the quest of many authors in analyzing threats faced by organizing information and ways to curb this ugly art. Though every many organizations' information might be of importance but the health care information cannot be compromised because it is only one life exist for every individual, and [1, 2] viewed health care sector as most complex business endeavor with different kinds of interaction. On the other hand Meanwhile [3] exert some characteristics of a healthcare sector that makes it a business organization as having a business resource (time, people, money and business processes) to manage, a large staff and staff payroll, serves as a market where demand and supply takes place, and produces a large cash flow. [3] Highlights that the healthcare sector is a business because: It manages the same set of business resources as other types of organizations, including financial resources, personnel, equipment, supplies, technology and facilities. It employs a large complement of staff and has a large payroll. It serves as a marketplace and supplies valuable services to hundreds of customers daily. It procures a vast array of supplies, both pharmaceutical and technological. Time, people, money and business processes are managed to function efficiently. It is an economic engine that generates significant cash flows and provides economic value. Organizations are more vulnerable to insider attack since it is unlikely to be detected at the early stage. Moreover, with the readily available authorized access and knowledge about the imperfection of the system [4, 5, 6, 7], such attack can be easily launched once tempted employees are presented with the opportunity [8]. At this point, health organizations one of the most important sectors that must be maintained their hospitals' information system security [9]. These organizations contains sensitive data concerning patients, any malicious action to destroy this system affect the reputation or the lives of human beings, as well as intellectual and material losses [10]. On 2007 special investigation by The Times newspaper [11], it was reported that the medical record of Dr. Manto Tshabalala-Msimang, Minister of Health in

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

South Africa from 1999 to 2008 under President Thabo Mbeki, was stolen from the private clinic where she was admitted. It was then passed on illegally to a news reporter, who used it to write an article by Sunday Times that exposed the minister's behavior when she was admitted to the clinic. That caused a scandal and harmful to the Minister of health.

The primary objective of this paper is to investigate deeply the human factors that compromise an information system's security in terms of insider threat. And to figure out what are the meaning of malicious human factors and what is the reasons to cause threat act to the patients personal information in Iraq hospitals and what is the most influential factors among them, notwithstanding [12] opinion, i.e., "*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.*" Some organizations have failed to recognize such disaster [13, 8] that may befall when the employees are tempted to steal, destroy, or leak sensitive data because of personal vengeance, monetary gain, or to demonstrate their loyalty to third parties, ingratiation, coercion, thrills [14]. However previous studies have not been realized of all employees within the organization. While studies have been conducted on the (managers and employees) separately. Have not been addressed in one study. Most of the studies used survey method and self-reported data. The limitation of self-reported data was unavoidable, thus the reliability of self-reported data is tenuous. In addition they turned to focus on policies and some security measures, followed inside the organization. But the problem lies in human behavior accurately and their motivations to blow their malignant actions. This study covered all the internal officers (managers and employees) and focuses on peer-reported data or officers-observed data to validate the results which include the managers and the employees.

This paper is organized into five sections. First section starting with introductory of research problem, second section is an overview of literature, followed by the third section is research methodology and the tools that used for analyzing the results, then the fourth section we present the findings of this research, and finally in the fifth section we discuss the findings with the limitation and future work.

2. RESEARCH BACKGROUND

Insider threat originates from legitimate personnel who exploit their familiar environment and system for personal gains. Even though the occurrence of such internal attack is not as frequent as external attacks, it is more likely to succeed and bring devastating effects. According to the annual Computer Crime and Security Survey CSI/FBI survey results spanning eight years from 2000 [15], the reported incidents of internal attacks and insider abuse have topped the chart. The following sections give a clear picture to understand the internal threats, and who are cause these threats and what are the incentives for these threats.

2.1 The Insider Threat is Occurs

Insider threat refers to an individual with legitimate rights and authorization having the capability, motivation and opportunity to violate security and harm a business or an organization [16]. As a matter of fact, insider attack is most commonly launched by employees seeking revenge or financial gains, and such malicious insiders "plague" the employers who have employed them with good intentions [17, 18]. They prey on the loop holes in the security system that has been created by chance or due to ignorance. In this aspect, the Computer Security Institute's survey that was conducted in 2008 revealed that almost 44% of all organizations have experienced computer system abuse. However, this number has been decreased to 30% in 2009. In addition, in 2008 and 2009, approximately 42% of organizations reported some cases of laptops loss and 17% of them reported customers' data robbery [15]. The results of a survey in 2009 [19] also indicate that 25% of the respondents who participated in the study believed that insiders were responsible for almost 60% of the financial losses. They also believed that insiders have unauthorized (or privileged) access to almost 15 % of organization facilities. Moreover, the fourth most frequent event is insider's abuse of internet access and e-mails. The results of both studies revealed that the threat of insiders is a fact to be considered. Further, this threat is increasingly turn into an external threat level. The following figure 1 illustrates some examples of the insiders' threats.

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

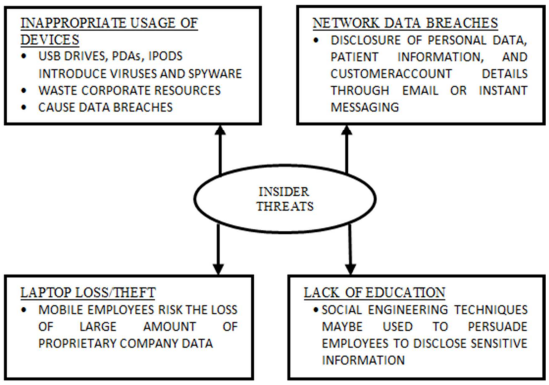

Figure 1: Insider Threat [16]

Based on the results of study for 500 or more patient reports, published by Department of Health and Human Services, over sixteen million person have been affected because of their information security breach [20, 9]. Another study published by PricewaterhouseCoopers [21], it has been reported that about 42% of organizations are not totally aware of the source of incidents, implying the fact that they do not know whether the origin of attack was employees (either current or former), customers, partners, suppliers, hackers, or others. Besides, if no incident occurs, organizations have generally no idea whether insiders may be stealing or destroying information. I n this regard the next sections classify the insider threat factors.

2.2 Insider Threat Factors

To clearly understand the concept of an 'insider threat', it is first essential to identify the elements that constitute the threat. In general, the threat of an insider may be intentionally, accidentally or due to ignorance [22]. Each type of insiders' threats includes threat agents who are representative of an individual or group manifesting a threat [23, 24]. Based on "Threat-agent relationship" by [25], such agents have the following features in order to be a threat for an organization, an insider threat agent must have the capability, motivation, access to resource, opportunity, catalyst, inhibitors and amplifiers. These three components clearly discussed as the following:

Threat Capability: The main components of capability required for an insider to be capable of making a threat for the organization have been pointed out by [26]. In fact, the effectiveness of insider's attack highly depends on the insider threat agent's capability i.e. the higher the capability is, the greater the threat would be [24]. It means that the agent has a great opportunity to attack and maintain the attack and destroy any replacements as well. In order to fulfill any attack, the agent requires the capability such as resources, knowledge, technology, and etc.

Threat Motivation: An insider threat agent's motivation is ranged from idle curiosity to malicious intensions. [25, 27, 2] summarizes different elements that motivate an insider agent to threat the organization. It is important to know that each employee in an organization may be a potential threat if they have the motivation to capitalize on their capacities and the opportunities they may have as they work in the organization [28]. The personal gain, revenge, competitive advantage, ideology or even a combination of them may be the underlying elements to evoke a malicious insider's motivation.

Threat opportunity: In order to execute an attack on the organization, an insider with the capability and motivation would need the opportunity to do so [29]. In this respect, [25], demonstrates the elements that create opportunity for an insider's attack. The threats include misusing a user's account or using a valid user's account logged on in an unattended workstation. The insider can make a copy of sensitive documents, when the user is absent.

2.3 Categorizing Insiders

In any organization or business, each employee has a specific access level, which is based on his job profile. In addition, any other third party like clients, contractors are also provided with specific levels of access. In the current study, insiders are generally categorized as pure insider, insider associate, insider affiliate, and outside affiliate. It should be mentioned that this classification is based on the one made by Dr. Cole and Ring – authors of the book "Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft" [30]. The different groups of threat agents are categorized in the following figure 2.

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

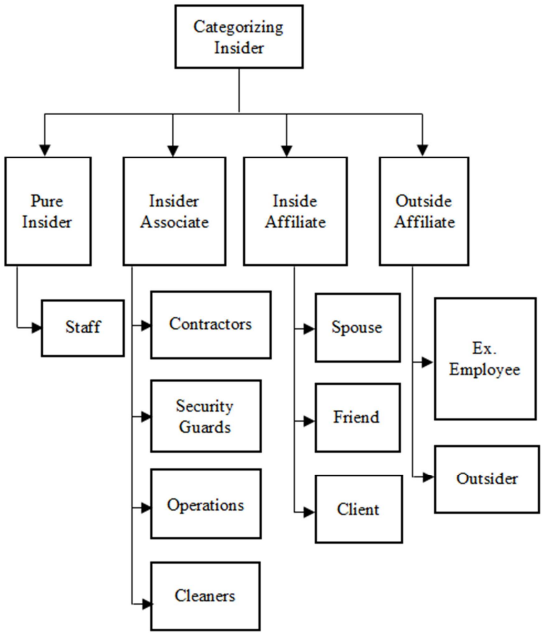

Figure 2: Categorizing Insider [30]

A pure insider refers to an employee that is entitled to access the organization and its system for job purpose, though the entitlement is most of the time limited according to his or her job role. System administrators, on the contrary, have full access to the systems and networks, and thus, present a greater threat when he or she launches an attack. Ironically, employees that have left the organization, regardless of their job roles, do not have their accounts deactivated. This, in fact, poses a threat to the security of the information systems and networks. The Insider associate refers the third party personnel like guards, cleaners, suppliers, and etc. as well as contractors that support the operation of an organization with restricted access to its facilities, systems, and/or networks. These personnel may advocate insider attack, especially after office hours, when they have unlimited access to the pure insiders' work stations to retrieve sensitive information and/or documents without any surveillance. For example, collecting the username and password from a piece of post-it note attached to the cubicle. The affiliate of an insider includes the immediate family members, friends, and clients who are not authorized to access any system or network in the organization, but are able to launch an insider attack through the pure insiders' credentials. This may come in a form of becoming an imposter to access the facilities, systems, and/or networks which includes, for instance, using the employee access card to enter the organization's premises. And finally the outside affiliate are the unknown personnel who are not trusted by the organization, and thus are not allowed to retrieve any information through open access. However, with enough technical knowledge, they are able to initiate an encoded attack. The most obvious example is the hackers.

2.4 Preliminary Research Model

Based on the many different research studies by many scientists on the impact of human factors on the information security of an organization, it has been found that majority of the attacks are initiated by dissatisfied employees who are seeking revenge or tempted employees who are looking for financial gains, and thus triggered an insider 'plague' [16], .The abuse of system access and privileges are common. Most insider attacks generally start with abusing the system, and then violating security policies [31], according to the 2010 survey [32] 72% of the insider incidents are handled internally. Cybersecurity Watch Survey, [32]. An insider threat agent's motivation is ranged from idle curiosity to malicious intensions. Summarizes different elements that motivate an insider agent to threat the organization. It is important to know that each employee in an organization may be a potential threat if they have the motivation to capitalize on their capacities and the opportunities they may have as they work in the organization. The personal gain, revenge, competitive advantage, ideology or even a combination of them may be the underlying elements to evoke a malicious insider's motivation [25, 22]. Based on the studies that mentioned above and other exploratory researches [8, 33, 34, 22] there are six personal characteristics believed to have positive direct implications for threat act from insider lead to risk of hospitals' information system that contains patients' personal information [35], in this regard figure 3 shows the hypotheses in form of research model and the following hypotheses was proposed:

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

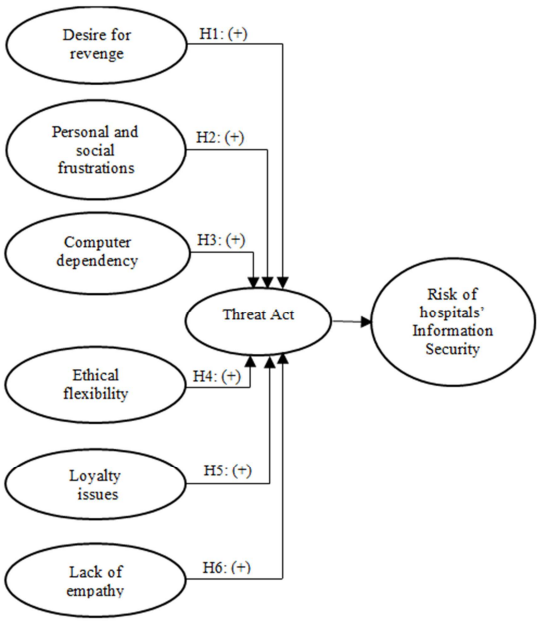

Figure 3: Proposed Research Model

2.5 Hypotheses Development

According to figure 3. The hypotheses that proposed they were configured as a research model of this study to present the malicious human factors which is widely previewed in the following sections:

H1: Desire for revenge is positively related to threat act.

The human malignant act by some of the employees, generated by a motivation or a certain belief to attack their organization's information system, in an intention of revenge from some colleagues. One of the reasons that some of the staff believes that their colleagues is not respect or detract them which will generate hatred. [36]. In this regard [37] refer that the weak link in an organization is the behavior of internal officers and their thoughts, [38, 39, 16] proved in their studies that desire of revenge can cause a big harm to hospitals information system.

H2: Personal and social frustration is positively related to threat act

To find out why employees may attack their organizations, to know when will be the attack, the link between potential attacks and malignant that may be behind some of the beneficiaries of access to personal data and disclosed, purpose behind it. There are factors which must be considered such as personal and social frustration and some other factors [25, 40, 41, 22]. The anger, alienation, and hatred lead to malignant behavior and reflect badly on the organization [27, 29] also pointed that personal and social frustration that the social environment in which the employee came from, affect the behavior inside the organization, one of the most important factors of hatred. According to [42, 43, 2], most studies refer that hatred of authority, tension and correlation these factors with anger, which is an important motivations in turn leads to the malignant behavior. [44] Suggests "trusteeship", meaning that the director or officer must be the guardian of the organization, and is aware for a malicious behavior of some staff, but unfortunately, this concept does not exist in some of them. In this regard [45] indicated that the workers will lead to many incidents inside the organization.

H3: Computer dependency is positively related to threat act

Unauthorized access to the organization information system and the computer devices to the rapid development in all areas of technology, which is a human challenge to break this technology [25, 46, 47]. [48], most managers trusts the technology, the problem lies in the users of these technologies inside the organization, and the employee is considered the main threat to the organization information system [8]. In this regard [28] refers to some of the staff who has the desire to detect encrypted symbols, motives either a personal reflection of some malicious behaviors or by poverty is the exploitation of some workers to break the codes and steal information and the desire to challenge the information security measures. Advances in technology and offers many of the devices, leading to ease of movement and the workers opportunities to attack their organizations in this regard indicates that the organization should not rely on computers only [48].

H4: Ethical flexibility is positively related to threat act.

The side of moral and ethics, which the staff professional and moral character and not tamper with the security of information that may lead lives of humans, confer a few other factors, a sense of

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

responsibility in case some of the workers know that their staff within the organization has intentions to attack or harm to their organization or has already happened, but nevertheless do not take any action or report that malignant behavior [27, 2] pointed that the workers ethical lead to the failure of the organization if was bad. Ethics flexibility factor in study of [49,50, 51, 8] , shows a positive effect lead to threat act on information system, insider risk can made a strong damage for organizations information system. Some employee they can threat the organization information system for unethical reason, and lack of ethics by break the policies and rules can cause a disaster for the organizations [8]. [49] Flexibility refers to the work ethic, and that many of the cases from previous studies confirmed that this aspect has led to significant damage in the information security. In this regard [25] refer that the insider they have the capability to sabotage organizations information system. [49] indicates that the human factors aspect of this type is unintentional and, in turn poses a real danger to the security of information.

H5: loyalty issues is positively related to threat act.

The conflict between the employers, competition, dissatisfaction, and some workers are unhappy with his work. These factors affect the loyalty of employees to their organizations and become the focus on self-interest and loyalty to himself which reflect a bad behavior [52, 53]. The insiders they have the capability for any malicious behavior [54] and they ease to betrayal their organization [25, 40, 48, 8]. [50] A large part of insider threat adopted by trust and loyalty. systematic thinking to get out of this organization and to discuss these with responsible persons from outside the organization, leading to make way for two more to break this person through this gap, because this person behavior is not carrying the loyalty of his work [2].

H6: Lack of empathy is positively related to threat act.

The lack of interest and sympathy with the staff by business managers and by colleagues at work, this factor leads to low self-esteem and mental illness, the employee leads to a reaction against the organization, and this is not the right of employee to combine the work with the integration of personal [8, 55, 16]. The insider they are a big challenge for any organizations [56], throughout the ages we see that the staff at least sympathy with the progress of time and this is due to fatigue at work and dealing with many cases leading to a lack of interest in working and abnormal behavior [54]. [25] refer that the insider they always have the intention and the motivate to attack the organization information system.

3. DATA COLLECTION

The researcher conducted our surveys at the 5 major publicly held hospitals in Iraq, survey samples were written in English and then back-translated into Arabic to ensure conceptual equivalence and comparability, all participants in our surveys were familiar with the hospital information system (IS). All of the surveys were conducted in the hospitals during the work time and the completed questionnaires were taken directly by the researcher early of 2013. All participants were assured of the confidentiality of their response before beginning the survey. The descriptive statistic used to describe the basic feature of the sample and shows the frequency distribution and histogram of the demographic variables, including gender, position, education, department, age, and years of experience. This kind of analysis helps us to know the respondent has adequate knowledge about risk in hospital. Initially 400 questionnaires were distributed to the internal officers, 301 completed questionnaires were valid. we tested the Normality to check the distribution of data to make sure to use parametric or non-parametric test and we tests the Reliability, composite Reliability to check the reliability of questionnaire and the Factor Analysis to extract the factors, for this purpose each factor value is calculated by calculating the average of answer of each person to the related question to that factor and correlation to check the relation between the factors. We designed a questionnaire that was commensurate at the Iraqis' health sector, we validated and refined the measurement scale of the proposed model, for an effective response scale ranging from 1 (''strongly disagree'') to 5 (''strongly agree''). The partial least squares (SmartPLS 2.0) technique, which is a structural equation modelling technique, was applied to data processing. The PLS is widely used for empirically-base studies due to its appropriateness for small sample sizes, and modelling and validating predictive models [57]. Importantly, PLS supports the assessment of both a measurement model and a structural model. Data analysis proceeded in a two-step approach recommended by [58]: (1) an

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

analysis of the measurement model was conducted which aims to evaluate reliability and validity of the measures and (2) testing of structural relationships among latent variables followed.

4. FINDINGS

4.1 Descriptive Analysis

The results of the descriptive analysis are used to describe the basic feature of the sample. The descriptive analysis show the frequency distribution and histogram of the demographic variables, including gender, position, education, department, age, and years of experience. This kind of analysis helps us to know the respondent has adequate knowledge about risk in hospital. Depict the demographic characteristics of the study participants. Of the 301 respondents. 193 were male and 108 female, representing 64.3% and 36.7% respectively. 25.7% of the respondents aged 20 to 29-year-old. The number of 30 to 40-year-old respondents was 117, which made up 38% of the entire respondent population. The third largest respondent group, constituting up to 22.7% of total respondents, aged 40 to 49-year-old. 12.3% of the respondents were in the 50 to 59-year-old age range while the remaining 1.3% was made up of respondents aged 60-year-old and above. On the other hand, most of the respondents, i.e., 33%, had a bachelor degree, 16.7% were diploma holders, 14.71% were doctors of philosophy, 13.7% held a master's degree, and the rest were higher diploma holders. Furthermore, 46.7% of the respondents were doctors, 23.3% were nurses, 15% were staff managers, 7.3% were employees, and 7% were managers. The departments being surveyed were ENT, Accouter, Research, Optometric, Orthopedics, and Pediatrics. Most respondents were either from the surgical (17.3%) or medical (16.7%) workforce. Lastly, 30.7% of the respondents had one to five years of experience while 25.7% of them had 11 to 15 years of experience. Based on the demographic information we understand this study covered all the internal officers in Iraq hospitals with all departments inside the hospitals and the power of collected data come from the well-educated of the respondents. 70% of them are graduates of universities and a large number of them higher degrees that reflect with the understanding of the importance of this study. In addition 73% of them in middle age that give good experience to understand the importance of information system security. On the other hand 68.7% of respondents are managers and doctors that's give more confident to collect data in such like this environments.

4.2 Research Model Measurement

4.2.1 Multicollinearity Estimation for Formative Construct

Multicollinearity test is to limit if the variance inflation factor (VIF) < 3.3 [59]. Examine multicollinearity in case if the model having both reflective and formative constructs [60]. We then measure collinearity issue by testing the value of tolerance and VIF. The maximum VIF value for item is 1.289 for Personal and social frustration when as threat act chosen as dependent variable and minimum one is 1.122 for computer dependency while lack of empathy is 1.169, refer to Table 1 for construct VIF , Tolerance value and indicators weight. The results support that the formative measures of uncertain factors are reliable and valid. These values of VIF is less than 3.3 which mean it is strongly acceptable [59].

Table1: Formative Construct measurement

indicator	weight	Tolerance	VIF
Social and Personal Frustration			
Q5	0.630	.104	1.289
Q6	-0.099		
Q7	-0.138		
Q8	0.340		
Q9	0.441		
Computer dependency			
Q10	0.252	.161	1.122
Q11	0.542		
Q12	0.614		
Lack of empathy			
Q21	0.125	.189	1.169
Q22	0.481		
Q23	0.767		
Q24	0.181		

4.2.2 Validity and reliability for reflective constructs

Convergent validity were used to assess the construct validity of the instruments used in this study. According to [61] construct validity is essential to ensure that a set of items actually represents the theoretical latent construct these variables were designed to evaluate. In addition to the standardized factor loadings in the confirmatory factor analysis, convergent validity in the present

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

study was examined by observing the value of composite or construct reliability (CR) and average variance extracted (AVE) for each construct. As noted by [61], CR values should be greater than 0.6 while AVE should be above 0.5. CR value that is lower than 0.6 indicates that the items do not consistently measure the hypothesized latent construct and the value of AVE that is smaller than 0.5 indicates that more error remains in the items than variance explained by the latent factor structure imposed on the measure [61]. The results of loading, AVE and CR are shown in Table 2. These results supported the convergent validity of each of the constructs involved in the proposed hybrid model of this study.

Table 2: Reflective measurment constructs

Indicator	Loading	AVE	Composite Reliability
Desire of revenge			
Q1	0.729	0.545	0.782
Q2	0.737		
Q3	0.750		
Ethical flexibility			
Q15	0.647	0.648	0.781
Q16	0.937		
Loyalty issues			
Q17	0.503	0.531	0.812
Q18	0.689		
Q19	0.719		
Q20	0.939		
Threat act			
Q25	0.612	0.530	0.769
Q26	0.831		
Q27	0.724		
Risk of hospitals' information systems'			
Q28	0.755	0.565	0.796
Q29	0.743		
Q30	0.759		

Here, the reliability test was utilized in order to verify the consistency of the measurement scale for each construct and to purify the results via a reliability coefficient. Internal consistency of the measures exists if composite reliability (CR) and item loadings of each criterion exceed 0.7 [62]. All the values for internal consistency are met. The assessment of this validity is completed by using bootstrapping method to test t-values, and path coefficients for each construct and verify whether significant or insignificant these tests clarified in section 4.3.

4.3 Hypotheses and structural model Testing

With regarding to the evaluation of the proposed model, we evaluated path coefficients (the coefficients of the relationships between variables), to figure out if the hypotheses that proposed would support the research hypotheses or not support. We performed hypothesis testing by following [57] and the significance of each paths coefficient estimated by t- test using bootstrapping with 5000 subsamples. The result of hypothesis testing including, t-value, p-value and β are indicated in Table 3.

Table 3: Results of hypotheses testing

Variables	t-value	p-value	path coefficients β	R^2	Hypotheses
Desire of revenge	3.893	0.000***	0.232		Supported
Personal and social frustration	2.225	0.026*	0.141		Supported
Computer dependency	2.865	0.004**	0.170		supported
Ethical flexibility	3.046	0.002**	0.179		Supported
Reduced loyalty	1.863	0.063	0.130		Not Supported
Lack of empathy	1.010	0.313	-0.067		Not supported
Threat Act				0.246	
Risk of Hospitals' Information Security System				0.232	

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

According to table 3, desire of revenge has a positive influence on threat act construct was fully supported (β=0.232, T-value= 3.893). The result shows that desire of revenge is significantly related to the risk of hospitals' information system. As well as the personal and social frustration has a positive influence on threat act construct was fully supported (β=0.141, T-value= 2.225). This result also explains that the personal and social frustration is significantly related to the risk of hospitals' information system. It shows that there is a relationship between personal and social frustration and threat act. The empirical evidence of the computer dependency has a positive influence on threat act construct (β= 0.170, T-value= 2.865). Suggested that computer dependency factor is also related significantly with the risk of hospitals' information system Also the relationship between ethical flexibility and threat act construct (β=-0.179, T-value= 3.046) has a positive influence and it is significantly related to the risk of hospitals' information system. But we cannot claim the positive relationship between loyalty issues and threat act, because (β=0.130, T-value=1.863) shows that in this case loyalty issues has not a direct strong relationship with threat act. The result shows that loyalty issues is not significantly related to the risk of hospitals' information system .The empirical evidence (β=-0.067, T-value= 1.010) shows that the lack of empathy has no influence on threat act construct. Thus, the hypothesis regarding the direct impact of threat act is not valid. In addition, examining the impact of threat act on risk of hospitals' information system, for the proposed hypotheses were found to be true. R-square scores for each dependent construct shows the percentage of construct's variance: Threat act (R^2 =0.246) which represent about 24% of the variation in threat act is explained by the six malicious human factors, while 23.2% of the variation in the risk of hospitals' information system is explained by the model (R^2 =0.232).

As shown in figure 4, the model was tested by performing bootstrap approach to evaluate t-statistics [63] of the linkage. the two- tailed t-value is conducted at 1.645, 1.96, and 2.576 critical values of "t" at significant level (p-value) 0.1, 0.05, and 0.01 respectively [64].

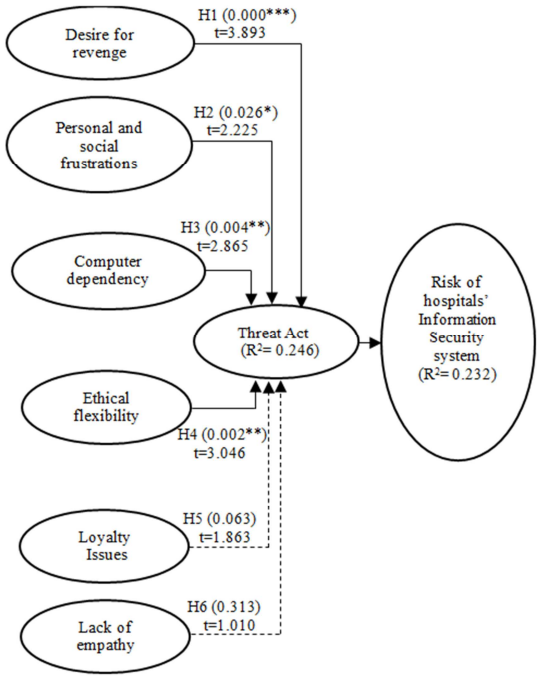

Figure 4: Structural model of hypotheses testing
**Significant at 0.05 level **Significant at 0.01 level ***Significant at 0.001 level*
- - -► *Insignificant path*

5. DISCUSSION AND CONCLUSION

The purpose of this study is to examine the influential variables that affect the hospitals' information system security. The proposed model subject to statistic testing is based on literature review, the results was interesting to observe that two hypotheses related to ''malicious human factors'' (H5 and H6) are not significant and not valid. Our analyses show that ''loyalty issues, and ''Lack of empathy" do not influence perception of ''threat act'' of risk of hospitals' information system which previous literature review strongly found to be significant and a positive influence on threat act and have relationship on the risk of hospitals' information system. This finding contradicted to the significant positive relationship suggested by previous studies. One possible explanation of the resulted insignificant relationship may due to the inaccurate measure of perceived social pressure, or belief based measurement approach may provide more accurate measure by first identifying the accessible referents, i.e., the people whose opinions are important to the surveyed person as a sensitive information. An

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

alternative interpretation of the insignificant relationship for computer dependency construct may not be a direct determinant of the intention to perform security breach it could be resulted due to adverse information security incidents and the ignorance of using the technology in time that most managers trust the technology, the problem lies in the users of these technology inside the organization. And there is a possible explanation regarding the lack of empathy construct that is the concept of "threat act" on risk of hospitals' information system security doesn't have relationship with the sympathy of the employees to their organization or another possible explanation is the employees' estimation of the value, sensitivity or importance of the organizational data was not merely based on monetary evaluation. The hypotheses (H1, H2, H3, H4) proposed positively have impact on risk of hospitals' information system security in this study shows that the variables desire of revenge, personal and social frustrations, computer dependency and ethical flexibility positively influence on threat act construct and significantly related to risk of hospitals' information system security this findings is compatible with the previous studies.

Finally this research examined a comprehensive model of malicious human factors (see Figure 3) via surveying 301 respondents in Iraq hospitals'. This model is unique in the sense that it has been developed based on the data obtained from both field study and literature .The data were analyzed through structural equation modeling (Partial Least Square) approach. One of the most important findings was the identification of six-variables of insider threats to information system security. In the previous studies, researchers confirmed that all the tested variables it have significant impact on information system security (ISS). But this study brings out a new results and shows some variables have no influence on ISS, which reflects in new understanding for human behavior. Which represent some of malicious human factors as unintentional threat act, could be human errors, accidental incidents or ignorance. Another significant contribution of this research the results can help the Iraq hospitals to look deeply to the impact of insider threats, trying to avoid many cases of employee's abuses on their ISS, that's come from the practice and knowledge that they got from this study. The limitation of this study is the comparatively small sample size and the number of organizations. Another limitation of this study. The samples collected from health care/hospital organizations, which has special policies concerning the data is sensitive compared to other organizations. This research essentially examined the entire research model that has been given a very clear indication of what malicious human factors are. And examined which factor are more influential, also we identify how the malicious human factors could interrelate to each other. Sure, that serious series only captured after a certain amount of the view, but that this study have contributed to understanding why pretending the perspective. We have tested our knowledge using a survey of 301 people and that's can show the hypotheses panel is correct. Also, in order to further understand certain element that came up from the survey. Suggestion for the future study could be extracted and explore in detail and examine the factors individually. This study focused on the malicious human factors. In the future, it will be possible to compare between these factors and the organization's culture or the examination of these factors on the other organizations are not within the health sector.

REFERENCES:

[1] Gomes, R., & Lapão, L.V. (2008), "The Adoption of IT Security Standards in a Healthcare Environment", In S.K. Andersen, G.O. Klein, S. Schulz, J Aarts, & M.C. Mazzoleni (Eds.), eHealth Beyond the Horizon – Get IT There - Proceedings of MIE2008 – The XXIst International Congress of the European Federation for Medical Informatics (pp. 765-770). The Netherlands: IOS Press. Retrieved January 05, 2009, from www.hst.aau.dk/~ska/MIE2008/ParalleSessions/PapersForDownloads/10.Sta/SHTI136-0765.pdf.

[2] Debra Box, Dalenca Pottas (2013), "Improving information security behavior in the healthcare Context", Elsevier Ltd. doi: 10.1016/j.

[3] Langabeer, J. (2008), Health Care Operations Management: "A Quantitative Approach to Business and Logistics. Sudbury": Jones & Bartlett Publishers.

[4] Stanton, M.J., Kathryn, S.R., Mastrangelo, J.J. (2005), "Analysis of end user security behaviors", Computers & Security 24 (2), 124–133.

[5] Nash, K.S., Greenwood, D. (2008), "The global state of information security", CIO Magazine, PriceWaterhouseCoopers.

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Karin Hedström, Ella Kolkowska, Fredrik Karlsson, J.P. Allen (2011), "Value conflicts for information security management", Elsevier B.V. doi:10.1016/j.jsis.

[7] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinso, Cate Jerram (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", Published by Elsevier Ltd. http://dx.doi.org/10.1016/j.cose.2013.12.003

[8] Williams, P.A.H. (2008), "When trust defies common security sense", Health Informatics Journal 14 (3), 211–221.

[9] C. Derrick Huang, Ravi S. Behara, Jahyun Goo (2014), "Optimal information security investment in a Healthcare Information Exchange: An economic analysis", http://dx.doi.org/10.1016/j.

[10] Maseti, O. (2008), "A Model for Role-Based Security Education, Training and Awareness in the South African Healthcare Environment", In Academic Dissertation, Nelson Mandela Metropolitan University. South Africa.

[11] Maker, J., & Power, M. (2007), "Special Report: Manto Tshabalala-Msimanga - Top cop set on trial of Manto's missing medical file", The Times. Retrieved October 12, September 23, from http://www.thetimes.co.za/SpecialReports/Manto/Article.aspx?id=570532

[12] Gene Spafford (2007), "From Enemy at the Water Cooler: Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures".

[13] Meredith B, "Data protection and freedom of information", BMJ 2005; 330(7490):490–1.

[14] M. Keeney et al., Insider Threat Study (2005), "*Computer System Sabotage in Critical Infrastructure Sectors",* US Secret Service and CERT Coordination Center, Software Eng. Inst., Carnegie Mellon Univ., May 2005; www.secret service.gov/ntac/its_report_050516.pdf.

[15] CSI Computer Crime and Security Survey (2008), http://i.cmpnet.com/ v2.gocsi.com/pdf/CSIsurvey2008.pdf.

[16] Kuheli Roy Sarkar (2010), "Assessing insider threats to information security using technical, behavioural and organisational measures", Elsevier Ltd. doi:10.1016/j.istr.

[17] K.H.Guo, Y.Yuan, N.P.Archer, C.E.Connelly (2011), "Understanding nonmalicious security violations in the workplace: a composite behavior model", Journal of Management Information Systems 28 (2), pp.203–236.

[18] Princely Ifinedo (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", Elsevier B.V. http://dx.doi.org/10.1016/j.im.2013.10.001

[19] CSI, CSI Computer Crime and Security Survey (2009), http://gocsi.com/survey.

[20] Kaufman Rossin & Co. (2012), "Hitech Act Three Years Later: Are Health Records Safe?" White paper Series.

[21] Safeguarding the new currency of business - Findings from the (2008), "Global State of Information Security Study", http://www. pwc.com/en_GX/gx/information-security-survey/pdf/ safeguarding_the_new_currency.pdf

[22] Federica Paci, Carmen Fernandez Gago, Francisco Moyano (2013), "Detecting Insider Threats: a Trust-Aware Framework", IEEE. DOI 10.1109/ARES

[23] A.Moore, D.Cappelli, R. Trzeciak (2008), "The Big Picture of Insider IT Sabotage Across U.S. Infrastructures", Advances in Information Security,Vol. 39, pp.17-52.

[24] N. Kanaskar, J. Bian, R. Seker, M. Nijim, N. Yilmazer (2011), "Dynamical System Approach to Insider Threat Detection", IEEE International Systems Conference (SysCon), pp. 232-238.

[25] Andy Jones & Debi Ashenden (2005), "Risk management for Computer security - Protecting Your Network and Information Assets", Elsevier ButterwortheHeinemann. ISBN: 978-0-7506-7795-0

[26] Rhee HS, Cheongtag K, Ryu YU (2009), "Self-efficacy in information security: Its influence on users' information security practice behavior", Computers & Security: p. 816-826.

[27] Workman M, Bommer WH, Straub D. (2008), "Security lapses and the ommission of information security measures: A threat control model and empirical test", Computers in Human Behavior. p. 2799-2816.

[28] Hui-wen Tang, Anlin Cheng, Chong-Cho Chang (2013), "Insider trading, accrual abuse, and corporate governance in emerging markets — Evidence from Taiwan", Elsevier B.V.http://dx.doi.org/10.1016/j.pacfin.

[29] Beaudry A, Pinsonneault A. (2010), "The Other Side of Acceptence:Studying The Direct And Indirect Effects Of Emotions On

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Information Technology Use", MIS Quarterly.34(4): p. 489-710.

[30] Dr. Eric Cole, Sandra Ring (2006), "Insider *Threat - Protecting the Enterprise from Sabotage,* Spying, and Theft", Syngress Publishing.

[31] Verizon Business Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf; 2009.

[32] Cybersecurity Watch Survey, CERT, http://www.cert.org/archive/pdf/ecrimesummary10.pdf; (2010),

[33] Coulehan J. (2010), "On Humility. Annals of Internal Medicine".153(3): p. 200-201.

[34] Posey C, Bennett RJ, Roberts TL (2011), "Understanding the mindset of the abusive insider: An examiniation of insiders causal reasoning following internal security changes", Computers & Security: p. 486-497.

[35] Carroll, R. (Ed.). (2004), "Risk management handbook for health care organizations", (4th ed.). San Francisco, CA: John Wiley & Sons, Inc.

[36] Shaw E, Post J, Ruby K. (1999), "Inside the mind of the insider, security management".

[37] Odlyzko, A. (2003), "Economics, Psychology, and Sociology of Security", Available at http://www.dtc.umn.edu/publications/reports/2003_07.pdf

[38] Marianthi Theoharidou (2005), "The insider threat to information systems and the effectiveness of ISO17799".

[39] Williams PAH (2007*), "Medical data security: are you informed or afraid?"* International Journal of Information and Computer Security 2007b; 1(4):414–29.

[40] Eric D. Shaw (2006), "The role of behavioral research and profiling in malicious cyber insider investigations". 1742-2876, Elsevier Ltd. All rights reserved, doi:10.1016/j.diin.2006.01.006.

[41] Carl Colwill, Laura Pritchard (2009), "*Human factors in information security: The insider threat-who can you trust these days?"* Elsevier Ireland Ltd. All rights reserved. doi:10.1016/j.ijmedinf.

[42] Lee, J. and Y. Lee (2002), "A Holistic Model of Computer Abuse within Organizations." Information management & computer security **10**(2): 57-63.

[43] Schultz, E. E. (2002), "A Framework for Understanding and Predicting Insider Attacks." Computers & Security **21**(6): 526-531.

[44] Willison R. (2006), "*Understanding the offender/environment dynamic for computer crimes",* Information Technology and People.

[45] Campbell, K., L. A. Gordon, et al. (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", Journal of Computer Security **11:** 431-448.

[46] Juanita I. Fernando, Linda L. Dawson (2009), "The health information system security threat lifecycle: An informatics theory".

[47] Moore AP, Cappelli DM, Caron TC, Shaw E, Trzeciak RF. (2009), "Insider theft of intellectual property for business advantage : a preliminary model", In: 1st International Workshop on Managing Insider Security Threats. West Lafayette, USA: Purdue University.

[48] Greenfield, S. (2007), "*Risky Thinking: Brain, Biology & Behaviour"*, IRM Risk Forum.

[49] Stanton, J. M., C. Caldera, et al. (2003), "*Behavioral Information Security: Defining the Criterion Space",* Symposium presentation at the meeting of the Society for Industrial and Organizational Psychology, Orlando, FL.

[50] Hamilton S, Micklethwait A. (2006), "*Greed and corporate failure: the lessons from recent disasters",* Basingstoke, UK: Palgrave MacMillan.

[51] Edward Humphreys (2008), "Information *security management standards: Compliance, governance and risk management"*, Published by Elsevier Ltd

[52] Farahmand F. (2009), "Insider behavior: an analysis of decision under risk", in: 1st International Workshop on Managing Insider Security Threats. West Lafayette, USA: Purdue University. p. 22e33.

[53] Jorge Blasco, Julio Cesar Hernandez-Castro, Juan E. Tapiador, Arturo Ribagorda (2012), "Bypassing information leakage protection with trusted applications", Elsevier Ltd.doi:10.1016/j.cose.

[54] Hongbin Zhang, Jianfeng M, Yinchuan Wang, Qingqi Pei (2009), "An Active Defense Model and Framework of Insider Threats Detection and Sense", IEEE.DOI 10.1109/IAS.

[55] Stephen H. Conrad and Felicia A. Durán, et al. (2003), "Modeling the Employee Life Cycle to Address the Insider Threat", System Dynamics Conference.

[56] Nesren Waly, Rana Tassabehji, Mumtaz Kamala (2012), "Improving Organisational Information Security Management: The

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Impact of Training and Awareness", IEEE.DOI 10.1109/HPCC.

[57] Wynne W. Chin (1998), "Issues and opinion on structural equation modeling", MIS Quarterly22 (1): 7–16

[58] Anderson, James C.; Gerbing, David W. (1988), "Structural equation modeling in practice: A review and recommended two-step approach", Psychological bulletin, psycnet.apa.org Vol 103(3), 411-423

[59] DIAMANTOPOULOS, A. & SIGUAW, J. A. (2006), "Formative versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration", British Journal of Management, 17, 263.

[60] Phatcharee Toghaw Thongrattana (2010), "Assessing reliability and validity of a measurement instrument for studying uncertain factors in Thai rice supply chain", SBS HDR Student Conference. http://ro.uow.edu.au/sbshdr/2010/papers/4

[61] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006), "Multivariate Data Analysis, sixth ed. New York: Macmillion Publishing Company", Chapter 8: Cluster Analysis.

[62] C.Fornell, D.F. Larcker (1981), "Evaluating structural equations models with unobservable variables and measurement error", Journal of Marketing Research 8 (1), pp 39–50.

[63] RINGLE, C. M., WENDE, S. & WILL, A. (2005), "SmartPLS 2.0". www.smartpls.de.

[64] WAGNER, S. F. (1992), "Introduction to statistics", New York: HarperPerennial.