THE INTERNATIONAL JOURNAL OF
SCIENCE & TECHNOLEDGE

The Security Mechanisms Put in Place against Insider Information Systems Security Threat in Public Universities in Kenya

Denis Wapukha Walumbe
Lecturer, Eldoret National Polytechnic Eldoret, Kenya
James Ogalo
Lecturers, Kisii University Kisii, Kenya
Jotham Waskie
Library Director, Kirinyaga University Kirinyaga, Kenya

Abstract:
Insiders are the people with legal access to the information and pauses a challenge to the security of the information systems. Public universities are facing serious insider security threats with several incidents being reported in internal security reports. The paper seeks to look at the current mechanism that public universities in Kenya have put in place when it comes to insider security threats. The objective was to examine the current mechanisms that the university has put in place to control insider security threats. Since it is evident that public universities have experienced insider security breaches, it is essential to establish the measures in place in dealing with the insider threats. Some of the issues that insiders pause for an organization is compromise the system security through misusing the resources they have been assigned to accomplish their roles in the university. There are models that have been presented to help organization protect itself against insider security attacks. The models presented are categorized as predictive, intent-driven threats models and domain-oriented model. However, public universities in Kenya are not using the models presented in prevention and prediction. They have the conventional access control using username and password which do not prevent insiders as they have legal access to the systems. They have implemented systems in place for external security threats but minimal control of the insider security threats. The study proposes a model that was modified to suit the public university environment and can be used for security threats prediction for the insiders.
All the abstract elements must be included:

Keywords: *Insider threats, security model, systems security*

1. Introduction

Institutions have always put forward the top-notch tools, procedures and policies in the process of protecting its information systems from attackers and infiltration from outside. Despite the amount of investment channeled towards development of infrastructure and manpower in guarding against the external aggressors, the universities still experience significant attacks causing greater loses. Though there are technical and physical controls deployed by institutions to manage access to certain restricted resources, these measures are reactionary, only taking effect when insurmountable damage has already been done. Thus, it can be argued that they come second after the human element. A network access security policy can only be followed by an employee who follows rules (Maasberg, Warren & Beebe, 2015). This is true for other technical controls such as log monitoring, firewalls, and honeypots among others.

A dissident employee will find a way to circumnavigate the security policy no matter how strict it might be. When dissidence occurs with respect to laid down rules and policies, the psychological settings of employee changes, subsequently jeopardizing productivity. According to Perlow, (2003), employee resentment leads to decreased productivity and creativity which ultimately leads to loss of money, time and resources. Many organizations relay the information that dissent is discouraged whether verbally or non-verbally. However, a number of studies have corroborated Perlow and noted that receptiveness to dissent facilitates design of corrective measures to monitor unethical employee behaviours, impractical and inefficient organizational policies and poor and unfavourable decision making processes. Leading among all is the chance dissent accords organizations to respond to insensitiveness to employees' occupational needs and requirements. Eilerman in Perlow, (2003) argues that the hidden overheads of silencing dissent include decreased job satisfaction and motivation reduced decision quality and lost time (Claycomb et al., 2014). According to Perlow, (2003), employee resentment leads to decreased productivity and creativity which ultimately leads to loss of money, time and resources. Many organizations relay the information that dissent is discouraged whether verbally or non-verbally. However, a number of studies have corroborated Perlow and noted that receptiveness to dissent facilitates design of corrective measures to monitor unethical employee behaviours, impractical and inefficient organizational policies and poor and unfavourable decision making processes. Leading among all is the chance dissent accords organizations to respond to insensitiveness to employees' occupational needs and requirements. Eilerman in Perlow, (2003) argues that the hidden overheads of silencing dissent include decreased job satisfaction and motivation reduced decision quality and lost time (Claycomb et al., 2014).

Objective of the paper is to look at the security mechanisms in put in place against insider information systems security threat in public universities in Kenya. The purpose is to look at the security threats prevention models that universities are using to protect the information systems resources from the insiders.

2. Literature Review

2.1. Classification of Security Insider Security Models

The current literatures have put more weight on the concept that information security is not an issue of technical measures (Carroll, Greitzer & Roberts, 2014). Information security is about the people, organizational factor, technology and the working environment. There are three types of security controls that have been proposed to deal with all aspects of information security:

Formal control this is about the organizational structure and an operation which ensures that there is proper conduct of business and minimizes the chances of an incident or an attack or at least reduces the impact. The control measures may include putting different departments for security and IT with clear roles of the departments to ensure proper control of the systems (Carroll, Greitzer & Roberts, 2014). Informal controls are just the organizational culture, value and belief systems on the institution. It is where an organization through the management has shared vision and contribution towards achieving the vision is done by all the members. The organizational members are committed to seeing the vision accomplished. Increased trust and awareness of security issues for information system are some of the approaches that can be used in creating informal controls (Carroll, Greitzer & Roberts, 2014).

Technical control it is the mechanism that gives protection to the information systems from any kind of attack or incidents. The organization can use recovery and analysis applications, access control mechanisms, use of antivirus software among other mechanisms (Maasberg, Warren & Beebe, 2015; Melara et al., 2003).

Although each of the above control is important, they must complement each other (Carroll, Greitzer & Roberts, 2014). The search study by Martinez-Moyano et al., (2008), confirms that successful defense against the insider threats demands that technical and behavioral solutions be implemented.

2.2. Prevention Detection and Responses to Insider Threats

There are other ways in which controls or measures are classified apart from formal, informal and technical controls (Schultz, 2002, Carroll, Greitzer & Roberts, 2014).

Prevention, it is a measure aimed at removing any chances of occurrences of an insider threat. It includes measures which can be able to predict the insider attacks by looking at the potential indicators. As per Carroll, Greitzer & Roberts (2014) government agency regulatory forces the organizations to come up with such risk management methods. The internal security policy that for regulatory compliance and insider prevention, the internal policy behaviour and actions those employees in the organization should adhere to. But if the policy itself has limitations where it is not enforced with strong consequences then it is not useful. The consequences are important in keeping away insider threat (Carroll, Greitzer & Roberts, 2014).

Detection it is a measure that offers means of knowing that there is an insider threat when it has already happened. There are several tool and methods for outsider attacks detector where insider attack occurrence is not easy to detect (Carroll, Greitzer & Roberts, 2014). The insider can delete the actions to cover up the illegal actions carried out which makes it difficult to detect (Carroll, Greitzer & Roberts, 2014). Tools such as logging, honey pots, monitoring and whistle blowers are being implemented.

Response is another measure that is expected to detail how to respond after the insider attack has actually happened. The institutions are expected to take responsive actions against the insiders. It may be a simple solution of lawsuit for the company. In reality, it is not simple to respond to insider threats with lawsuits. The need for organizations to keep such events from public eye or bad press is what results dealing with the issues internally (Carroll, Greitzer & Roberts, 2014). There are many lawsuits where the organization is not likely to recover the damages but only punish the insiders. Although such actions may seem good in the public eye, recovering of lost assets, bad press and effects on stock market for publicly listed company is not possible (Carroll, Greitzer & Roberts, 2014).

Although detection of insider threats just like the external threats is more preferred, in nature it is a post hoc approach (Schultz, 2002). According to Schultz, the most pressing need is developing a framework for predicting insider attacks. This is the aspect that the research seeks to address the urgent need of developing a model. There are several indicators discussed which can be modelled into a framework that can be used to predict insider attack.

2.3. Prediction Model

Wang, Liu and Zhang (2006) proposed a model for prediction of the insider threat using a tree structure (2006). The authors used in their paper the attack tree that was introduced by Bruce Schneier (1999) in defining their model. The attack tree can be used for both internal and external attacks. The scholars came up with the Systems Attack Tree configurations after analysis of all the attack paths in the system in order to detect the insider threat.

The insiders who take advantage of the information system weakness on the security policy or measures are the insider threats. Security policy on the other hand is aimed at reducing the weaknesses that results into the system risk of information misuse. In the end the security policy may present weaknesses that lead to other risks[1] .

The scholars state that if we are able to understand the intents of the insider access to the internal resources, then it is possible to intercept and detect insider threat. The insider offers reasons for access to the system before being allowed to access the system. The table known as the Signature Powered Revised Instruction Table (SPRINT), is set and the system makes Agent Observes (Aos), that is the operations the insider would like to perform in the system based on the SPRINT plan. The Minimal Attack Tree generated by Aos is used to make security systems detection of the malicious intent. The figure below shows the setup for insider detection.

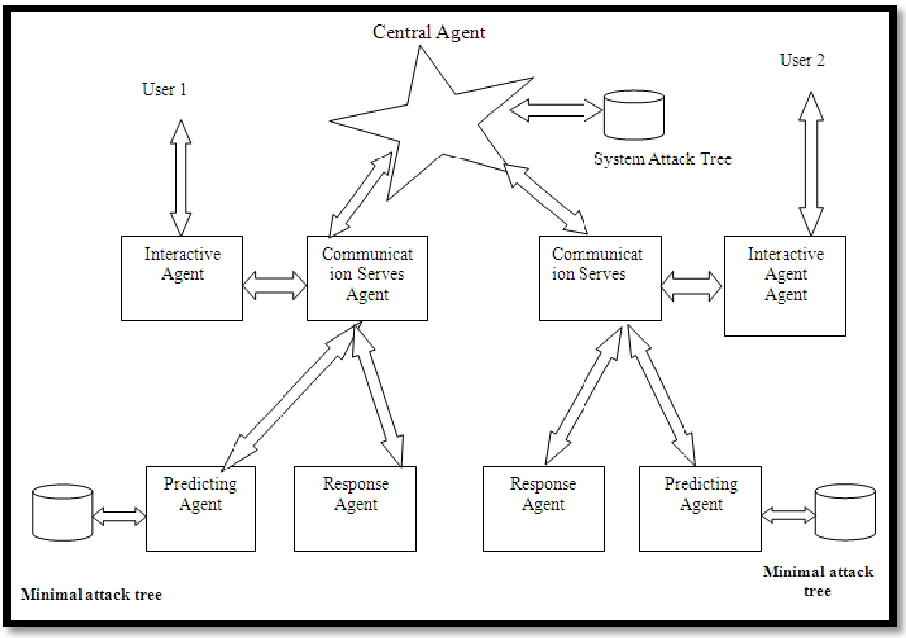

Figure 1: Framework of Insider Threat Model
Source Liu and Zhang, 2011

From the **Error! Reference source not found.** above, at the time of connection to the system by the insider, there are interactive agent requests for information on why the user has to access the resources and the n users have to wait for some time. The systems give information to the user after configuration the Central Agent generates the Minimal Attack Tree after making a comparison with the System Attack Tree. The Prediction Agent Observes the behaviour of the user by the Minimal Attack Tree to analyse the chance of attach. The user behaviours are stopped if the system detects any malicious intent.

2.3.1. Domain Oriented Approach

Qutaibah and Panda (2008) presented a domain-oriented approach in predicting and mitigating an insider threat (Qutaibah and Panda, 2008). The approach presented states that the internal resources that an insider can access is denoted by s, where the insider can take more organization information. Access to company information gives the insider a chance to access confidential information, if the insider has malicious intent. The authors states that the knowledge that the insider has on how to access confidential information need to be controlled.

2.4. Intent-Driven Insider Threat Detection

Santos et al., (2008) presented an intent-driven framework that has s users of the model and insider detection metrics. The model automatically detects the insider threat (Santos et al., 2008). Although the traditional studies on insider threats have put more weight on social network, document based and action based, the researchers focused on understanding the intent of the user.

Users have intention whenever they access the internal resources be it malicious or not. For one with malicious intent, there are some features that the mode presents (Santos et al., 2008) such as use of many queries that are not supported, use documents that are old when there are no supporting documents, fabrication of information; when making reports and overstating some of the record information. It is through experiments that the insider intent is understood and classified accordingly.

The authors used the IPC model 1 (Nguyen et al., 2004b; Santos et al., 2003a) in coming up with the framework that contains the list of interest, preference network and context network. The context network is most critical one. The document graph (DG) is used to model the knowledge context of the user.

[1] ISO/IEC 15408, 1999

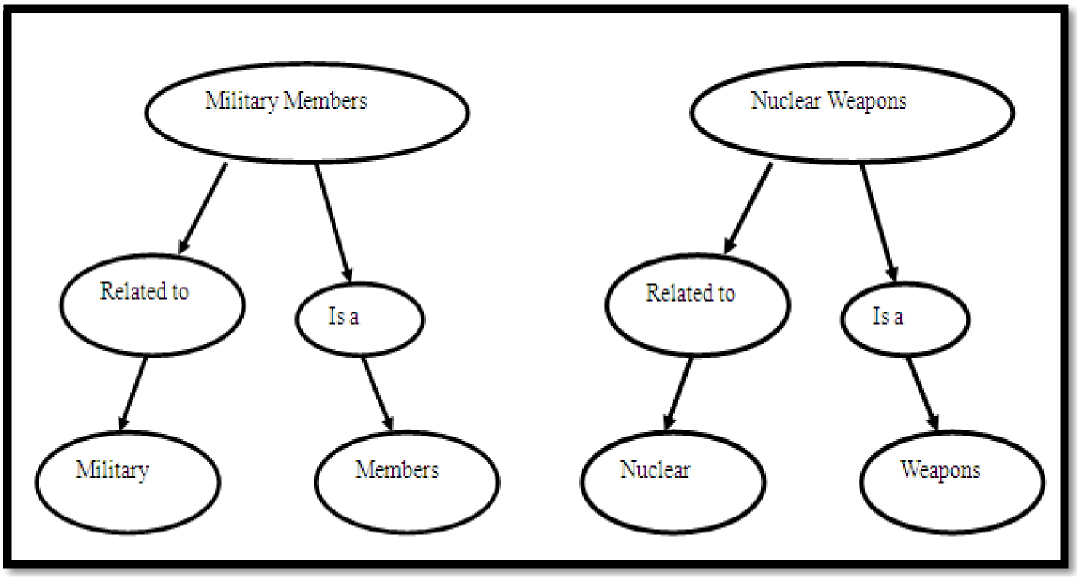

Figure 2: Example of Document graph
Source: (Montes-y-Gómez, Gelbukh & Lópes-López, 2000)

From the figure 2.4 above DG example, there are nodes and relationship between the nodes. There are two types of relationships 'Is a' relation and 'Related to' relations. The similarity between the documents accessed and the context network is computed using the following equation (Montes-y-Gómez, Gelbukh & Lópes-López, 2000):

$$\text{similarity}(DG1 + DG2) \quad = 1 + \frac{n}{2N} + \frac{m}{2M}$$

Where
n is the number of concept nodes as shared by DDG1 and DDG2
N is the total number of concept nodes in DG1
m is the number of relation nodes as shared by DDG1 and DDG2
M is total number of relation node in DG1

2. Methodology

Quantitative research methodology was used in the study. In Kenya, universities are mainly categorized into public and private universities. The public universities are under the government management under the ministry of higher education.

2.1. Research Design

Research design is important because it tell the readers the approach used in collecting data and hence the findings of the study. This study used quantitative approach. One of the reasons for choosing quantitative design is that they provide an actual bottom-line or dollar amount of the associated costs making them appealing in terms of non-technical decision-making processes (Creswell et al., 2003). Quantitative models designed for information security analysis are mostly specific to organizational contexts. In this case it was suitable in the context of public universities in Kenya. The target population for the study was the two public Universities in Kenya. The university employees especially those with access to information systems were the main target of the study. Therefore, actual population in this study that was established and accessed was as follows: information systems users, information system security policy enforcers, ICT experts, and heads of departments. Stratified random sampling was used to get the representation of the two strata of Kibabii University and University of Eldoret. The technique is more suitable since it reduces the sampling error and improves the representation of the sample (Hair et al., 2010). Simple random sampling was used after stratification of the sample to get proportionate representation of each strat

2.2. Factor Analysis

Total Variance Explained									
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulativ e %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulati ve %
1	3.452	28.764	28.764	3.452	28.764	28.764	3.229	26.912	26.912
2	1.512	12.596	41.360	1.512	12.596	41.360	1.493	12.442	39.354
3	1.317	10.973	52.333	1.317	10.973	52.333	1.435	11.955	51.309
4	1.130	9.420	61.753	1.130	9.420	61.753	1.204	10.035	61.344
5	1.035	8.629	70.382	1.035	8.629	70.382	1.085	9.039	70.382
6	.805	6.710	77.092						
7	.710	5.913	83.005						
8	.678	5.650	88.656						
9	.536	4.469	93.125						
10	.455	3.793	96.918						
11	.274	2.283	99.201						
12	.096	.799	100.000						

Table 1: Total Variance Explained
Extraction Method: Principal Component Analysis

Factor analysis was carried out to extract various mechanisms that are being used in guarding against insider security threats in public universities. The method of extraction was Principal Component Analysis. Kaiser recommends that factors with eigen values greater than 1 should be retained. Five factors with eigen values greater than 1 were extracted and it accounts for about 70% of the variability in the original variables. The table above shows the factors that were extracted, factor loading and rotation factors presented.

Rotated Component Matrixa					
	Component				
	1	2	3	4	5
Trained by the university on security protection methods for information systems	.927	.052	-.030	-.031	.081
Trained regarding password strength, complexity and scheduled changes?	.823	-.067	-.093	-.173	-.081
Strong and mandatory password change after a period of time	.726	-.158	.061	.025	.146
Frequency of change your password	-.217	.594	-.386	-.182	-.126
Give sensitive or confidential digital information to county or state regulators without proper authorization	.023	-.169	.710	.060	.208
Discuss or disclose sensitive or confidential digital information during personal conversations while at work	-.506	.564	-.067	.224	.156
Discuss or disclose sensitive or confidential information with non-employees while away from work	-.042	-.085	-.015	.908	-.030
You aware of methods external system attackers can get confidential digital information from you	-.913	.101	.046	-.201	-.026
The university trained you how to recognize a legitimate warning message	.071	.039	.106	-.005	.902
I manually lock your computers when you are away from your desks	.026	.799	.102	-.082	.016
The institution allows you to install programs on the university computers	.130	-.044	-.652	.390	.016
Institution has a well-accepted "Bring Your Own Device" policy in place	-.055	.320	.560	.250	-.388

Table 2: Factor Loading For Mechanisms against Insider Security
Extraction Method: Principal Component Analysis
Rotation Method: Varimax with Kaiser Normalization
a. Rotation Converged in 7 Iterations

The table above is the rotated matrix table using Varimax with Kaiser Normalization. It gives how individual factor relates with the component. The component with values higher than 0.6 is regarded as with high relationship with the component since variance is high. The score is measure from 0 to 1 where scores close to 0 are weak relations and those close to 1 shows strong correlation.

Factor	Item	Factor Loading	Mechanism Name
1	Trained by the university on security protection methods for information systems	0.927	Information Security awareness
	Trained regarding password strength, complexity and scheduled changes?	0.823	
	strong and mandatory password change after a period of time	0.726	
2	Discuss or disclose sensitive or confidential digital information during personal conversations while at work	0.564	Manage organizational culture
	I manually lock your computers when you are away from your desks	0.799	
	you aware of methods external system attackers can get confidential digital information from you	0.101	
	Frequency of change your password	0.594	
3	Institution has a well-accepted "bring your own device" policy in place	0.560	Information Security policy
	Give sensitive or confidential digital information to county or state regulators without proper authorization	0.710	
4	Discuss or disclose sensitive or confidential information with non-employees while away from work	0.908	Access control and authentication
	The institution allows you to install programs on the university computers	0.390	
5	The university trained you how to recognize a legitimate warning message	0.902	Physical access control

Table 3: Factor and Mechanism Used in Public University

The literature groups the security mechanisms into informal, formal and technical mechanism. The grouping below shows that public universities use a combine of the mechanisms as categorized below.

- Security awareness- security awareness or education is often seen as one of the mechanisms that institutions use is protecting the systems. Training of the information users on security protection methods, trained regarding password strength and strong and mandatory password change. The factors are training of employees on the methods of protecting the information systems and the need of having a strong and period change of password.
- Manage organizational culture- this is a mechanism that is aimed at having a culture which protects the information and related resources. Ensuring that information users do not disclose information while away from work and having a policy on how users can access critical resources are key mechanisms captured as factors in the above table.
- Security policy- there is a security policy in place for protection of the information systems. It is a mechanism that can be used in against insider security attackers. The factors in this mechanism are disclosure of confidential digital information during personal conversations and installation of programs on university computers. If the information system can install programs then they have administrative rights and it can affect the security of the information system.
- Authentication and access control- the two mechanisms have been combined although in literature they are explored separately. Training on password strength and recognizing legitimate warning message are part of access control while manually lock of the computer access control mechanism.
- Physical access control- remote access is accessing the systems away from the university premises and giving information to regulators without authorization is about physical access control mechanism.

3. Findings

This review on literature has touched on different key areas that the researcher thought is significant value to contribute to insider security mechanisms in higher learning in Kenya. This included insider security giving the understanding of what which the insider is, the insider threats, the motives of insider security attack. Different information security and how it is handled at various institutions, different models in place and the polices that need to be adapted by the institutions of higher learning. Practically, there are near-infinite employee types in an organization that a model should protect against hence nearly impossible. The models presented in the study are designed for a specific purpose and cannot be used in any industry. The literature identified several mechanisms that are being used in other institutions to counter insider security threats; the study divided the measures into technology, personnel and procedures or processes. The respondents were asked to what extent they agree or disagree with the statements on some of the practices and mechanisms in place for security measures against insiders. There were elements dropped after pilot study and the remaining elements are in the questionnaire for information system users from question 6-18

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.709
Bartlett's Test of Sphericity	Approx. Chi-Square	607.148
	Df	66
	Sig.	.000

Table 4: KMO and Bartlett's Test

The Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy was carried out and it indicates the proportion of variance in the variables that might be caused by the underlying factors. The KMO value for instruments was 0.709, which was acceptable as the middling value (Kaiser, 1974). Additionally, Bartlett's test of sphericity tests for the hypothesis that the correlation matrix is an identity matrix was done. The test was significant which means that the variables are unrelated and therefore unsuitable for structure detection. The Bartlett's test shows that there is statistically significant level hence the variables were accepted for further study.

4. Conclusion

There are no a lot of data about insider security attack hence there are inadequate approaches of measuring the aspect of insider security threat. Mainly institutions that have been victims of insider security have concealed such cases because of the sensitive nature. Currently, most of the researches are still in progress on the prediction models and most of the insider security solutions in existence are based on research. However, the current security solutions presented are not satisfactory like the external security solutions. The problem with insider security solutions is that the insider has an information, access and skills together with understanding of the organizational structure with knowledge of internal system security. It is difficult to protect the internal resources using the approaches discussed in the above sections. It is very difficult to use the system administrators to protect internal resources. It is because the system administrators, who have access to all system resources are as well as insider security system, may have malicious intent. They are the biggest insider threat. This creates the need to look at a model that is predictive. The model should not detect what has already been done but be able to tell us what is likely to take place and be able to secure the systems before it happens.

5. Recommendations

The study recommends the implementation of security models for prevention and prediction of insider information systems security threats. The current approaches are mainly used for preventing the university information systems resources from the external attacks. However, there are inadequate models or mechanisms being used for insider security threats. Designing a model for predictive and detection of insider security threats activities is recommended for public universities.

6. References

i. Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., & Center, C. I. T. (2012). Chronological examination of insider threat sabotage: preliminary observations. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3(4), 4-20.

ii. Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., & Center, C. I. T. (2012). Chronological examination of insider threat sabotage: preliminary observations. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3(4), 4-20.

iii. Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: detecting the insider threat through examination of dark triad personality traits. In 2015 48th Hawaii International Conference on System Sciences (pp. 3518-3526). IEEE.

iv. Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008). A behavioral theory of insider-threat risks: A system dynamics approach. ACM Transactions on Modeling and Computer Simulation (TOMACS), 18(2), 7.

v. Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., & Cooke, D. L. (2003). A system dynamics model of an insider attack on an information system. In Proceedings of the 21st International Conference of the System dynamics Society (pp. 20-24).

vi. Montes-y-Gómez, M., Gelbukh, A., and Lópes-López, A. (2000). Comparison of Conceptual Graphs. In Proceeding of MICAI-2000, In 1st Mexican International Conference on Artificial Intelligence

vii. Nguyen, H.; Santos, E Jr.; Zhao, Q.; and Wang, H. (2004b). Capturing User Intent for Information Retrieval. Proceedings of the 48th Annual Meeting for the Human Factors and Ergonomics Society (HFES-04), New Orleans, LA. Pages 371- 375

viii. Perlow, M. (2007). Managing Hedge Fund Conflicts of Interest,". Rev. Sec. & Commod. Reg., 40, 75-77.

ix. Qutaibah A., & Panda, B. (2008) Performance analysis of an insider threat mitigation model. ICDIM: 703- 709

x. Santos, E, Nguyen, H.; Zhao, Q. & Wang, H (2003a). User modelling for intent prediction in information analysis. Proceedings of the 47th Annual Meeting for the Human Factors and Ergonomincs Society. Pages 1034–1038.

xi. Schneier, B. (1999). Attack trees. Dr. Dobb's journal, 24(12), 21-29.

xii. Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526-531.

xiii. Wang, H, Liu, S, & Zhang, I (2006). A Prediction Model of Insider Threat Based on Multi-agent. 2006 1st International Symposium on Pervasive Computing and Applications.