International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

Identifying the Psychological Indicators and Mitigation Techniques To Reduce Insider Threats

[1]T. Kirthiga Devi,[2]Prof. S. Rajendran
[1]MTECH-Information Security and Cyber Forensic,SRM University
[2]Department Of Information Technology,SRM University.

.

Abstract — **Threats from the insider are difficult to identify and resolve because of true nature of the action. In protecting the integrity of our systems and data against insider threats is to monitor network access, the database for unusual activity, especially important and critical. The proposed framework will focus on monitoring the activities of internal users and predicting their next activities to provide real time or near real time alerts on violation or other suspicious activity. It will provide a detailed statistics on defining and capturing the relationship between elements for instance, how the insider's psychological state will impact with their motivation on attack using statistical model. Statistics of past attacks, for how often individuals have exhibited a particular set of attributes and resultant outcomes, is used to determine whether an insider would involve in malicious activity and the attack patterns. The framework may then allow experts to infer the risk associated with observing a series of states within the system.**

Index Terms — **Psychological Indictors, Bayesian Network, Model, Parameters.**

I. INTRODUCTION

Government and corporate organizations face a growing threat of malicious employees who steal confidential information, destroy information systems and can go unnoticed for months or even years. These threats often happen without warning and can cause enormous damage. After the fact, however, a pattern or trail can often become evident that could have identified the malicious insider. In most cases, this trail is a combination of suspicious activities (e.g., downloading big files after work hours) paired with a motivational or psychological profile (e.g., by having financial and personal stress) that indicate the desire to commit a malicious act This paper defines a Bayesian network model that incorporates psychological variables that indicate degree of interest in a potential malicious insider. The framework begins by identifying psychological variables hypothesized to characterize a malicious insider, as well as the relationships between these variables. The initial relationships are derived from the psychological literature and integrates these indicators

I. RELATED WORK

There has been much research into the psychology and motivation of insiders, but the fact remains that it is difficult to predict who will commit security fraud. This applies the methodology of conventional criminal profiling to computer

crime. Specifically, the model focuses on insider attacks and prescribes an organizationally-based method for prevention. The utility of this model is two-fold in that it: 1) allows assessing an incident or attack using profiling in addition to the usual technical tools, and, 2) provides organizations a way to evaluate/enhance their security processes and procedures from a human perspective .

Procedural steps in generating a profile: 1)A thorough analysis of the type/nature of the criminal act is made and it is then compared to the types of people who have committed similar crimes in the past**,** 2) An in depth analysis of the actual crime scene is made, 3) The victim's background and activities are analyzed, to look for possible motives and connections 4) The possible factors for the motivation of the crime are analyzed, **5)**The description of the possible offender is developed, founded on the detected characteristics, which can be compared to with previous cases.

Evaluating through Bayesian network model : A Bayesian statistical model was developed to model user behaviour where invalid user behaviour is determined by comparing user current behaviour with their typical behaviour and comparing their current behaviour with a

set of general rules governing user behaviour formed by system administrators. This prediction model has provided results that are very close to the actual user behaviour with obvious similarities between results and actual data. The results were improved after applying intervention mechanisms.

1) METHODOLOGY

This detection framework involve in discovering step by step procedure to identify insider threat. The model also defines relevant types of insider attack-related behaviours and symptoms—"indicators" that include deliberate markers, meaningful errors, preparatory behaviours, correlated usage patterns, verbal behaviour and personality traits. From these sets of indicators, clues can be pieced together to predict and detect an attack. The presence of numerous small clues necessitates the use of quantitative methods; multiple regression equations appear to be a particularly promising approach for quantifying prediction.

Procedure For Detection

Framework: The procedure for detection framework involve in following step process, [1] Identifying the psychological indictors of

an insider misbehaviour by evaluating the test cases got from an organization along with known indictors. The organisation may be IT/Non-IT companies ,[2] Evaluating each and every indictors respective to test cases
helps to determining the rank
(Disgruntlement: 0.58) through different
statistical models ,[3] Monitoring and
updating the database of an employee

-activities in a timely manner will help an organization to alert, prevent and predict about developing insider crime. Table 1: Indicates the psychological indicators and examining the observable way each factor correlated with the indicators. The observed pattern that are relationally correlated with-following descriptions, without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail. Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties. Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information. Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted. Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel Short trips to foreign countries for unexplained or strange reasons. Unexplained affluence; buys things that they cannot afford on their household income. It shows an unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships. They focus on Concern that they are being investigated; leave straps to detect searches of their work area or home; searches for listening devices or cameras. Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

Psychological Indictors	Observable way
Psychiatric Problem on Judgement	□ Problem with task performance □ Social interaction impacting to perform the job □ Knowledge of psychiatry treatment
Personality , Social and Decision Skill that increase in conflict & isolation	□ Difficulty in getting along with others □ Feeling of being above everyone □ Characteristics increase in disgruntlement
Previous Violation of rule	□ Financial Issues □ Security Interest in breaching
Personal Issues	□ Financial Stress

	Family Conflicts Family Illness Personal Failures
Negative Feeling Attraction	Employee believe wrongful behaviour and unfair advantage are rewarded Lack of work rewarded, Hard work not rewarded
Track of Concerning Behaviour	Disagreement over ownership Fights over increase in salary Conflicts in re allocation Being thirst of promotion but no work
Negative Feel Leads to stress	Believing co-workers and supervisors are about to harm my designation Feeling unreasonable anger and blame toward others.
Unusual Technical Behaviour	Unauthorized access Use of co-worker to achieve unauthorized access Anomalous copying or downloading especially prior to departure, travel, vacation, resignation, termination.

II. BAYESIAN NETWORK MODEL

Bayesian probability theory is a powerful technology for constructing models of phenomena involving uncertainty. Probabilities express degrees of plausibility or likelihood on a scale ranging from certainty through impossibility. Bayesian models will combine expert knowledge with observational data, and will be refined over time through learning from observation. Recently, a powerful new set of modelling methods has emerged that combine graph theory with Bayesian probability, enabling the construction of highly complex models involving large numbers of interrelated hypotheses. A *Bayesian network* encodes a probabilistic model over a set of related variables by using a directed graph to represent qualitative relationships and local probability distributions to represent quantitative information about the strength of the relationships. Bayesian networks will represent both causal and statistical dependency relationships.

Considering a set of variables to determine the risk value of psychological indicators, directed in acyclic graph representing two independent possible causes of a depicting the psychological indicators.P [Cause]

P [Indicators | cause] = P [Indicators | Cause] P [Indictors]

Any node in a Bayesian network is always conditionally independent of its all non-descendants given that node's parents. Hence, the joint probability distribution of all random variables in the graph factorizes into a series of conditional probability distributions of random variables given their parents. Therefore, we can build a full probability model by only specifying the conditional probability distribution in every node.

Indicators	**Prior**	**Weight**
Psychiatric issue on judgement	0.015	0.35
Social and Decision skill	0.015	0.42
Previous violation of rule	0.020	0.06
Personal Issues	0.020	0.80
Negative Feel of Interaction	0.036	0.15
Track of Concerning	0.042	0.25

Behaviour		
Unusual Technical Behaviour	0.015	0.15

1) CONCLUSION

To protect both employees and employers, systematic methods are needed to reduce the risk of deliberate attempts to harm corporate interests or individuals. The insider framework through the preponderance of reported case studies, the malicious intent of the perpetrator was "observable" prior to the exploit. We developed a prototype psychosocial model through behavioural indicators of increased insider threat risk. The combination of systems that monitor user cyber data on computer /networks and a system that records psychological indicators can provide in comprehensive solution to empower with a insider threat team with enhanced situation awareness. This will transform to reactive/forensics based approach in to proactive that will help identify employees who are at greater risk of harming the organization or its employees.

III. REFERENCES

1) S.R. Band, D.M. Cappelli, L.F. Fischer, A.P. Moore, E.D. Shaw, and R.F. Trzeciak, Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis (Technical Report CMU/SEI-2006-TR-026; ESC-TR-2006-091). CERT Program, Pittsburgh,PA: Carnegie Mellon University Software Engineering Institute, 2006.

2) S.S. Russell, M.J. Cullen, M.J. Bosshardt, S.E. Juraska, A.L. Stellmack, E.E. Duehr, and K.R. Jeansonne, Cyber Behavior and Personnel Security (Institute Report #661), Minneapolis, MN: Personnel Decisions Research Institutes, Inc, 2009

3) W.H. Hendrix, N.K. Ovalle, and R.G. Troxler, "Behavioral and physiological consequences of stress and its antecedent factors,"

Journal of Applied Psychology, vol. 70(1), 1985, pp. 188-201.

4) Identifying at risk employees: Modelling Psychosocial Precursor of Potential Insider Threat by Frank L.Gretizer,Lars J.Kangas

5) M. Mount, R. Ilies, and E. Johnson, "Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction," Personnel Psychology, vol. 59, 2006, pp. 591-622.

6) B.P. O'Connor and J.A. Dyce, "Tests of general and specific models of personality disorder configuration," in Personality Disorders and the Five-Factor Model of Personality, P. T. CostaandT. A. Widiger, Eds.Washington, DC: American Psychological Association, 2002,pp. 223-246.

7) S. Jakobwitz and V. Egan, "The 'dark triad' of psychopathy and normal personality traits,"

8) Personality and Individual Differences, vol. 40, 2006, pp. 331 – 339.

9) P.T. Costa and R.R. McCrae, Revised NEO Personality Inventory and NEO Five-Factor Inventory professional manual. Odessa, FL: Psychological Assessment Resources, 1992.

10) P. Barrett and P. Rolland, "The meta-analytic correlation between two Big Five factors: Something is not quite right in the woodshed," 2009. Retrieved on 1/12/2012 from http://www.pbarrett.net/stratpapers/metacorr.pdf.

11) In the model where perpetrators of computer crime and computer attacks is a psycho-dynamic driven model by Shaw, Ruby, and Post

12) D.M. Cappelli, A. Moore, and R. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), SEI Series in Software Engineering. Upper Saddle River, NJ: Pearson Education, Inc, 2012.

● ● ●