www.sphinxsai.com

ChemTech

International Journal of ChemTech Research
CODEN (USA): IJCRGG, ISSN: 0974-4290, ISSN(Online):2455-9555
Vol.10 No.5, pp 288-292, 2017

Behavioral analysis to minimize Insider threats –A technological perspective

Sreeja Swaminathan Puttan*, P Savaridassan

Department of Information Technology, SRM University, Tamilnadu-603203, India

Abstract : Minimizing insider threats require both technical and psychological approach. A security culture is required which include both approaches which helps in minimizing the risks to the organization. Strict behaviorists believed that any person can potentially be trained to perform any task, regardless of genetic background, personality traits, and internal thoughts (within the limits of their physical capabilities). It only requires the right conditioning. This paper aims to focus on different methods and the procedure to thwart insider risks caused by employees to organization.

Keywords : Behavioral science, psychiatry, insider threat, Psychological approach, Risk.

Introduction:

"The ability to mine data for nefarious behavior is difficult due to the mimicry of the perpetrator. If a person or entity is attempting to participate in some sort of illegal activity, they will attempt to convey their actions as close to legitimate actions as possible".[1]

"Organizational culture defines how an employee sees the organization. It is a collective phenomenon that is growing and changing over time and to some extent, it can be influenced or even designed by the management".[2]

"As the insider threats problem has grown, so to have the attention it has received within the research community. There have been in-depth discourses on everything from what exactly an insider threat is and what the range of human factor and psychological factors involved are, to how threats can be predicted, detected and effectively addressed with appreciation of technological and behavioral advances and theories".[3]

Much of the information related to insider threats resides in the relationships among the various entities involved in an incident. Culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues]. Security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture. Security culture should support all organizational activities in a way that information security becomes a natural aspect in the daily activities of every employee. A detailed background study would give a better picture on bringing out the leading aspects in the employee when applied reducing the human factor in causing internal risks to an organization.

Focusing on the technical aspects of security, without appropriate consideration of the human interaction with the system is evidently inadequate.

2. Methodologies:

2.1 The Morris water maze:

The Morris water maze (MWM) is a particularly sensitive task to examine age-related/AD-like deficits because it is highly specific for hippocampal function, one of the first and most affected brain regions in AD [4]. As a result, the MWM test is one of the most common behavioral tasks used to determine hippocampal spatial memory deficits [5]. The test consists of placing the rodent in a circular tank filled with cloudy water, which is used to motivate the animal to escape the water by swimming to a hidden platform located right below the water's surface. Over several days the rodent learns to find the hidden platform by using spatial cues, such as posters or taped objects strategically placed on the walls outside of the water maze, in the testing room. Distance swam, latency to reach the platform, and swim speed, most often recorded on video, are common measures of this test. The capacity of the animal to retrieve and retain learned information or the flexibility to purge and relearn new strategies can be determined using a probe trial and reversal trial. In the probe trial the platform is taken out and the animals are allowed to swim in the pool. Time spent in the region that previously contained the platform, crossings over the platform area, and time to reach the platform location are measured. The reversal trial is identical to the training trials, but in this case, the platform is switched to the opposite region of the pool, testing the cognitive flexibility of the animal that is necessary to relearn a new location. A cued version of this task, rendering the platform visible, can also be used to measure nonspatial strategies as well as visual acuity [6]. Variations include the radial arm water maze (RAWM) or plus-shaped water maze [7].

One desirable aspect of this task is that the motivating stimulus, i.e., escaping the water, does not require the food or water deprivation that is common in other spatial memory tasks. However, it has certain limitations as well, one of which is the fact that the various components of memory, i.e., reference and working memories, cannot be tested simultaneously.

2.2 Radial Arm Maze

One task that can accommodate simultaneous measurement of memory components and has also been widely used to study spatial memory performance in rodents is the radial arm maze (RAM). This maze consists of 8–17 equally spaced arms radiating from a central platform, which the rodent has to enter in order to attain a food or water reward placed in some of the arms. In this task, the animals guide themselves using spatial cues around the room, with the goal to enter each arm only once to receive the maximum amount of food or water rewards in the shortest period of time and with the least amount of effort. This maze requires the use of working memory to retain information that is important for a short time (within trial information), as well as the use of reference memory to retain the general rules of the task across days. Specifically, the animal must be able to remember which arms were baited as well as which it already entered (working memory), but it also must know to avoid non-baited arms across trials (reference memory), all of which takes place by being able to successfully encode spatial information. However, while this task permits the examination of both reference and working memory, major limitations are the use of food or water deprivation in this task, as well as the presence of odor confounds.

2.3 Passive-Avoidance Learning

In the passive-avoidance learning task, the animal must learn to avoid a mild aversive stimulus, in this case darkness, by remaining in the well-lit side of a two-chamber apparatus and not entering the dark where it receives the aversive stimulus. Note that since rodents innately gravitate to darkness, the animal has to suppress this tendency through pairing the negative stimulus with the desired compartment. Animals that do not remember the aversive stimulus will cross over earlier than animals that remember. Dependent measures include the median step-through latency (latency to cross into the unsafe side) and the percentage of animals from each experimental group that cross the threshold within an allocated time.

2.4 Core Belief Psychothreapy:

CBP is "talk therapy." It uses a highly specialized set of dialogue techniques and role-plays to correct Mistaken Core Beliefs. It does not involve hypnosis, digging for repressed memories, or anything that many clients see as "weird."

The CBP process allows therapists to do therapy at the core level (with the real self), and provide therapeutic experiences that convey worth and value while helping the real self to reinterpret negative childhood experiences. These therapeutic experiences correct Mistaken Core Beliefs, and bring the real self "back to life." This process leads to a profound sense of confidence, freedom, and personal power [8].

3. Behavioral Indicators:

Recognizing that behavior is something that individuals do, behavior analysts place special emphasis on studying factors that reliably influence the behavior of individuals, an emphasis that works well when the goal is to acquire adaptive behavior or ameliorate problem behavior. The science of behavior analysis has made discoveries that have proven useful in addressing socially important behavior such as drug taking, healthy eating, workplace safety, education, and the treatment of pervasive developmental disabilities (e.g., autism).

In the same way behavioral indicators indicate the nefarious activity of employees in the organization.

Few of the behavioral indicators are tabulated below related to information security.

Indicators	**Parameters**	**Data Source required**
Large Data transfers	File size	Email Gateway, DNS
Unauthorized removable media use	Transfer of data	MS Windows, Unix
Data alteration and deleting/wiping	Use of non-approved tools	MS Windows, Unix, network devices, document repositories
Attempts to access segregated/escalated systems/files/databases		MS Windows, Unix, network devices, document repositories
Transactional triggers on business systems	Business logic triggers that would capture misuse of access and rights	Network devices, Document repositories
Sensitive key word searching	Designated confidential or sensitive data	Network devices, Document repositories
Unauthorized user web activity	Monitor external internet activity and track access to black listed sites	Web proxy/next generation firewall, DNS, E-mail Gateway

Psychological Factors:

Some researchers have attempted to study the psychological profile of an insider who was likely to offend before the incident. Many researchers wanted to know how to spot potential insider attackers before they attack. However, for several years the criminal justice system has unsuccessfully sought to develop a profile of the internal threat criminal. Criminologists are not yet close to discovering criminals reliably in advance. Criminals differ in their motivations and psychological makeup. Thus, it should be possible to identify some types of very antisocial behavior, but it remains very difficult to identify other offenders because they can conceal themselves from advance detection. The presence of false positives obstructs these efforts. It is also difficult to identify internal threats in advance, because it is currently not possible to identify serious criminal intent or behavior. In addition, insiders' threat activity can gradually evolve from non-malicious intent to more malicious intent. A rigorous psychological evaluation might be sufficient to identify possible inside attackers while it might also prove to be offensive to the non-attackers who must be employed. Furthermore, the time spent to evaluate the candidate psychologically decreases the time available to consider if the employee would be beneficial to the organization or not.

As a result of this conundrum, even if a psychological exam existed its use might be counterproductive. The relative lack of cases to work with, the poor understanding of the best definition of average acceptable behavior, and the ambiguity in the identification of the boundary between acceptable and unacceptable behavior all combined to make the development of useful psychological profiles difficult [9]. However, Shaw, Ruby, and Post [10] assert that there are numerous features that, when found together, could indicate an increase in the possibility of harmful behavior on the part of the insider. These features are: computer dependency, a history of personal and social frustrations, ethical lapses, a sense of entitlement, and lack of empathy. Another major use for psychology is positive: the development of ways to supporting good behavior. Some researchers seek ways to use psychology to keep insiders acting in positive ways. The predictions look more hopeful for this use of psychology than for profiling. The difference between profiling and motivational methods is that profiling must be precise, producing few false positives and false negatives. The risk of a false positive is that of not employing a good employee or refusing somebody who has not yet demonstrated harmful behavior; the risk of a false negative is failure to detect or prevent an attack.

4. Experimental Analysis- Survey:

We have obtained data set through questionnaire based method. We have performed mistaken core belief analysis to detect the inherent attitude that may rise disgruntlement in the stakeholder.

Data *ANALYSIS* done to test Core belief of the individual are is tabulated as below:

Core belief	**% people who agree/believe**	**% people strongly agree**	**% people strongly disagree**
Powerless and cannot do much about their life	55%	10%	35%
Believe that their security is by depending on others	50%	35%	15%
Getting acceptance from others is very important	35%	35%	30%
Their worth is by their achievements and performance		70%	30%
Easily trust others	50%	10%	40%
Perfection	65%	25%	10%

The response rate was 100% as the assessment was conducted in hard copy sheets.

From the data which is been tabulated above, we have conducted reliability analysis and the ‘α’ value is 0.672. Which suggests that the questionnaire test has internal consistency of good value.Which in turn focuses on the fact that insider threat analysis has the human factor involvement that needs psychological assistance.

5. Conclusion:

Methods and data analysis though provide a probabilistic proof that insider threat minimization needs psychological assessment, there are few factors such as behavior analysis of the individual. Pattern based anomaly detection algorithm, network analysis though help in this but graph based detection algorithm must be developed to enhance the security culture in future which helps in minimizing the insider threats.

6. References:

1. William Eberle, Tennesse Tech University, And Lawrence Holder, Washington State University, “Detecting Insider Threats Using A Graph Based Approach”
2. Thomas Schlienger, Stephanie Teudel, University Of Fribourg, “Information Security Culture- From Analysis To Change”

3. Jason R.C.Nurse, Oliver Buckley, Philip A.Legg, Michael Goldsmith, Sadie Creese, Gordon R.T.Wright, Monica Whitty, Department Of Computer Science, University Of Oxford,"Understanding Insider Threat: A Framework For Characterising Attacks"
4. http://www.simplypsychology.org/biological-psychology.html
5. https://www.britannica.com/science/biological-psychology
6. https://www.ncbi.nlm.nih.gov/books/NBK5231/#ch1.s2
7. https://www.abainternational.org/about-us/behavior-analysis.aspx
8. https://www.ncbi.nlm.nih.gov/books/NBK5229/#ch4.s2
9. de Toledo-Morrell L, Morrell F, Fleming S. Age-dependent deficits in spatial memory are related to impaired hippocampal kindling. BehavNeurosci. 1984;98:902–907. [PubMed]
10. Ikegami S. Behavioral impairment in radial-arm maze learning and acetylcholine content of the hippocampus and cerebral cortex in aged mice. Behav Brain Res. 1994;65:103–111. [PubMed]
11. Morgan D, Diamond DM, Gottschall PE, et al. A beta peptide vaccination prevents memory loss in an animal model of Alzheimer's disease. Nature. 2000;408:982–985. [PubMed]
12. Lawlor PA, Bland RJ, Das P, et al. Novel rat Alzheimer's disease models based on AAV-mediated gene transfer to selectively increase hippocampal Aβ levels. Mol. Neurodegener. 2007;2:11. [PMC free article] [PubMed]
13. Vloeberghs E, Van Dam D, D'Hooge R, Staufenbiel M, De Deyn PP. APP23 mice display working memory impairment in the plus-shaped water maze. NeurosciLett. 2006;407:6–10. [PubMed]
14. de Toledo-Morrell L, Morrell F, Fleming S. Age-dependent deficits in spatial memory are related to impaired hippocampal kindling. BehavNeurosci. 1984;98:902–907. [PubMed]
15. http://www.core-beliefs-psychotherapy.com/
16. Pfleeger, C. P. 2008. Reflections on the Insider Threat. In Insider Attack and Cyber Security, ed. S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith and S. Sinclair, 5-16. Springer US
17. Shaw, E., K. G. Ruby, and J. M. Post. 2005. The insider threat to information systems1. the psychology of the dangerous insider. Security Awareness Bulletin, No. 2-98.

*****