International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 33 • 2017

Augment Information Security Culture Framework to Thwart Insider threat via lead Information Security Culture Framework

Sreeja Swaminathan Puttan[a] and P. Savaridassan[b]

[a]*M.TECH- Information security and cyber forensics*

E-mail : sreeja_swa@srmuniv.edu.in

[b]*Assistant professor, Department Of Information Technology, SRM University*

Abstract: Insider threat are the biggest threat to any organization. Though the world is being automatedwith the growing technology to ease human living, we, unknowingly setting a trap, which might get us doomed due to intentional and unintentional threats. Hence, it is important for us to build a security culture such that it would help us in protecting ourselves from technological sabotages and errors. This paper aims to present a psychological perspective on insider threat, where human involvement is influenced on information and communication systems in any organization.

Keywords: *Insider threat, Human Behavior, Psychological threat, Intentional threats, Information security*

1. INTRODUCTION

Leading aspects are interlaced with the core belief of an individual. Insider threats include both human and technological factor which stand against organizational information security. Threats that occur due by using technology, can be deterred. But just implying Information security policy, which cannot minimize the risks caused by intentional insider threats. Hence an information security culture which includes the shaping of core belief of the stakeholder should be designed such that human factor involved causing insider threat minimized minimizing the insider threat to an organization. An information security-aware culture framed with leading aspects will minimize internal threats to informationassets through the construction of appropriate inherent attitudethat guide employee behavior when interacting with information assets and informationtechnology systems.

The growing threat to all the organizations in the world is insider threat. An Insider threat is a threat caused by various factors. The factors may be due to the negligence of an employee or vengeance of an employee or any former employee of particular organization. Insider is the perpetrator or an actor who got irked by a situation of the company or an organization which convinces him to perform an act of sabotage or espionage. How well do we know the type of insiders?. We can differentiate them by the intention behind their action. Advertent Insiders are the insiders who sabotage the organizations reputation and push it into financial loss as vengeance. Inadvertent are those whose actions involuntarily results in risk to the organization. Since a decade Insider threat has been the biggest threat to the organization. While MOLE, recruited by a competitor of that organization to steal the confidential information for their own growth.

All the organizations has an organizational culture where security culture is a party of it. A security culture is a regime, where the things are done in a way to protect the intellectual property from competitors and physical or virtual damage.

Large, medium and small enterprises are interlinked as most of the projects are somehow outsourced to medium or small organizations. And according to the stats, small and medium enterprises (SME) are double in number than large enterprises.

Our research purpose is to establish a security culture in SME's or to enhance the existing security culture.

Few Informational security culture framework has been designed and been followed to protect intellectual property.

According to a survey done by a '*GARTNER',* 70% of the privilege escalations on sensitive data are done by the organization's employees. Destructing trusted information through secluded access, sending data via email and instant messaging apps, sharing information through peer-peer communication, offhand use of wireless networks, posting the information over social networking sites, sabotage, abuse of the business policies, photocopying or copy of source code for their own benefits, illegal alteration of product data.

It is important to understand that information security is not only related to information technology and communications systems field, but also falls under various sectors such as agricultural, banking, health and insurance etc.., Hence protecting data from various attacks is as important as protecting from insider threats.

2. RESEARCH WORK

Few indicators help us to identify the insider and type of attack. We differentiated them as psychological and behavioral indicators. Both though are similar, here we refer to actions over information and communication system by the stake holder of any organizations. We tabulated the behavioral indicators as follows.

Table 1
Behavioral indicators over ICT systems in any organization

Indicators	*Parameters*	*Source*
Un authorized Removable media use	Large amount of data sources being transferred	Ms Windows, Unix
Sensitive keyword searching	Business logic triggers that would capture misuse of access and rights	Network Devices, Document Repositories
Excessing printing	Exceeding 200 pages/day	MS Windows
Abnormal working hours	After hours and weekends Correlate with Badge + Mismatch	Badge card reader logs, MS Windows, Unix

Psycho logical Indicators : The indicators that indicate us the stakeholders' psychological state whether he is disgruntled, whether stakeholder is seeking vengeance towards the organization, is stakeholder a *MOLE*working for competitor.

A mole can be identified mostly through behavioral indicators over network by network based behavior monitoring. But sabotages are hard to identify. Hence we have decide to perform few assessments over three groups in three different organizations. Big five personality assessment, mistaken core belief assessment. CORE BELIEF assessment is required to minimize the insider threats. This is possible only if the stakeholders' inherent attitude is known. For future references we need to check the probabilities of disgruntlement too.

The psychological indicators that indicate an insider are disgruntlement towards the organization.

A stakeholder becomes perpetrator only if a situation has irked him. If management does not resolve it can become a major issue.

Prepared work: To thwart Insider threats we build a proactive measures which we refer as Lead Information security culture framework.

Lead Information Security Culture framework is theoretical approach to build a security regime for small and medium enterprises. Hence we have concentrated on few attributes that will help us building a lead information security culture framework to minimize the insider threat.

We have taken few attributes that acknowledge our research work in building a security culture. We have tested for the attributes using questionnaire method for the clues that attribute our factors for building the security culture. A human diamond factor with leading aspects have been taken as factors. While to attribute these factors we examine attributes from the questionnaire result.

Human diamond factor and leading aspects are Delight, Deliver, Develop, Depend, Society and regulations.

Scope we have using the five factors which are Strategy, Technology, Organization, People and Environment.

Strategy is the scope to check the implementation of different information security tactics such as security policy, guiding principle and priorities that are designed for organizational culture.Technology is the scope of security over hardware and software applications that are used in the SME's. Organization phase is apprehensive with the collection of information security beliefs, norms that significantly epitomize the organization. People is the attribute in the scope of information security framework, where stakeholder who are in direct and indirect contact with confidential assets of the organization. Environment is the factor where the detectable external elements nearby the organization that disturb its structure and operations and ultimately security of the information assets of the organization.

The third section in security framework implies change methodologies to thwart the risks caused by the employees of the organizations.

We have classified employees as inadvertent and advertent insiders for our convenience to apply the change management methodologies.

Refer the table below to understand the focus groups, training session like workshops and motivation and Knowledge repositories.

Game theory and Pattern based analysis are two major change methodologies which help management to identify clandestine user and naïve user.

3. CHANGE METHODOLOGIES

Game theory: Inadvertent or naïve users are the employees who are careless insiders, violate security policies or share sensitive information on social networking blogs. They need to be monitored to prevent insider threats. Game theory works on based on the incentives or appraisal given to the employees when they are constrained to work on projects with risk budget and security policy. They need to be monitored and negative or down in promised appraisal must be given but in a motivational way to support their effort and their noes must be noted. This must help them work under pressure without violating the policies within the risk budget.

Pattern Based detection: Pattern based method is a method where a pattern of work flow with possible scenarios will be designed. And employee is monitored to find out the outliers in the graph. If the work flow sample scenarios graph and the employee graph has any extra length or extra node added, then there is an anomalous behavior or action took place. Hence algorithm that detect anomalousbehavior will be advisable to detect the advertent insider in the organization.

Table 2

ISSUES: Human factor diamond and Leading aspects	*SCOPE*					*Change Management Methodologies*
	Strategy	*Technology*	*Organization*	*People*	*Environment*	
Delight, develop	Preparing employees to behave in a way such that they lead a secure manner towards organization and its assets					Focus groups
						Training sessions like workshops
						Expert training
Deliver/ responsibilities	Preparing employees to behave securely through effective monitoring					Motivation
						Knowledge repositories
						Pattern based analysis
Management/ depend	Ensure that employees are supported by management by showing effective management commitment, communication					Game theory
						Communication and management support
Society and regulation	Ensure that employees follow security policies and national culture. Consider external factors such as legal and regulation system					Culture analysis.

Approaches : Inherent attitude detection has been done for the research work. We are here, using the trade marked big five personality test and mistake core belief test. We will provide the test correlation test and analysis in the next section in detail.

BIG FIVE PERSONALITY TEST : The BIG FIVE PERSONALITY TEST is a questionnaire based assessment to test the five personality traits of an individual. The traits are openness to experience, conscientiousness, extroversion, agreeableness and neuroticism. Each trait depicts different attribute level of an individual. For our project we would be taking neuroticism, extroversion and conscientiousness into consideration.

MISTAKEN CORE BELIEF TEST : Mistaken core belief assessment is to assess the inherent attitude of the person based on self-confidence, trust worthy, cheat or abide by rules.

Techniques to reduce the human impact over insider threat are listed below.

Downward arrow technique: In this technique each individual will be under the supervision of a psychology expert where the psychologist rather questions him about the organizations environment, situations that rankles him. Undesirable instinctive thoughts which pops up and how far the stake holder’s critical thinking is helping him to cope up with the organizations culture. This will help him to look over the other possibilities in his career growth.

Core belief psychotherapy : CBP is “talk therapy.” It uses a highly focused set of dialogue techniques and role-plays to correct Mistaken Core Beliefs. It does not involve hypnosis.

The CBP course permits therapists to do analysis with the real self, and provide salutary understandings that express worth and value while helping the real self to reinterpret deleterious childhood experiences. These salutary experiences correct Mistaken Core Beliefs, and bring the real self .This process leads to a insightful sense of buoyancy, self-determination, which is one of our leading aspect for insider risk mitigation.

Experimental setup: This experiment for research has been done to detect inherent attitude and traits that indicate insider. This will be useful for us to minimize the human influence over cause of insider threat to organization. We have done the assessment using the questionnaire based analysis. A Likert scale has been considered to scale the questions in each test. They are calculated as per the instructions given in the assessment.

The traditional Cronbach alpha test using IBM SPSS software has been done on the data set obtained from three different organizations.The following table gives the result for the experiment where the considered traits are neuroticism, extroversion, conscientiousness from big five personality test. Threshold value for 'α' is **7** while **6** is acceptable.

Table 3
Reliability for conscientious ness

Reliability Statistics		
Cronbach's Alpha	*Cronbach's Alpha Based on Standardized Items*	*N of Items*
.810	.688	10

Table 4
Reliability for extroversion

Reliability Statistics		
Cronbach's Alpha	*Cronbach's Alpha Based on Standardized Items*	*N of Items*
.772	.613	10

Table 5
Reliability for Neuroticism

Reliability Statistics		
Cronbach's Alpha	*Cronbach's Alpha Based on Standardized Items*	*N of Items*
.720	.608	10

Cronbach alpha reliability has been suggestive and has been successfully resulted that give set of questionnaire were appropriate for the valuation of the context.

Ensuing table is the mistaken core belief data set obtained similar to the big five personality trait assessment.

Table 6
Reliability stating that trustworthiness

Reliability Statistics		
Cronbach's Alpha	*Cronbach's Alpha Based on Standardized Items*	*N of Items*
.872	.674	6

Table 7
Reliability for perfectionist trait

Reliability Statistics		
Cronbach's Alpha	*Cronbach's Alpha Based on Standardized Items*	*N of Items*
.768	.651	6

Let's see the response for the mistaken core belief assessment which helps in understanding the assessed attributes.

Table 8
The response for mistaken core belief questionnaire analysis

Core belief	*% people who agree/ believe*	*% people strongly agree*	*% people strongly disagreed*
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%

4. ANALYSIS

We interpret the data we obtained after analysis as follows. The assessment was done to find out the trait which results in insider threat.

From the analysis the dataset interprets that the possibility of human behavior over ICT system tend to produce threats such as sabotage, espionage, IP theft, Policy violations, Theft of Intellectual Tech, Damaging the source code. As the response has had us go all the round, few things are needed to be applied. We understand the possibilities of either of the insider threats mentioned are possibly not low.

Hence we need to build a security culture to minimize the insider threats.

5. RESULTS

An Information security culture for any organization is for the protection of their assets which includes sensitive data and their employees. Hence we, from the data obtained, interpretations stated above, advice to build an information security culture that has the leading aspects which put the stakeholder in the security culture regime frenzied.

6. CONCLUSION

The research sole purpose was to reduce the human factor in insider threat as it is higher and influensive over technology in organization. Few employment trainings and workshops, game theory would help in replacing the stakeholder in security culture track.

7. DISCUSSIONS

Advertent insiders cannot be minimized as they are intentionally cause harm to organization. Hence anomalies detection algorithm will help in detecting the advertent insider activity over network. Though we have to monitor verbal and cyber behavior to protect the organization from insider threats.

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://personality-testing.info/tests/IPIP-BFFM/

[5] https://understandingcbt.wordpress.com/tag/downward-arrow-technique/

[6] http://schoolnet.org.za/teach10/resources/dep/questioning/socratic.htm

[7] http://www.core-beliefs-psychotherapy.com/

[8] 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

[9] 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.

[10] 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]

[11] A. Da Veiga, N. Martins, and J. Eloff, "Information security culture-validation of an assessment instrument," South. African Bus. Rev., vol. 11, no. 1, pp. 146–166, 2007.

[12] .C. Chen, D. Medlin, and R. Shaw, "A cross-cultural investigation of situational information security awareness programs "Information Management & Computer Security, (16:4), pp. 360- 376, 2008.

[13] K. Parsons, A. McCormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security: Individual, Culture and Security Environment," Command, Control, Communications and Intelligence Division, Defenses Science and Technology Organization, Department of Defense, Australian Government. Australia, (2010).

[14] http://searchsecurity.techtarget.com/tip/Five-common-insider-threats-and-how-to-mitigate-them

[15] http://www.businesswire.com/news/home/20150618005371/en/3527623/Report-62-Cybersecurity-Professionals-Insider-Threats-Growing

[16] International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.163-178 http://dx.doi.org/10.14257/ijsia.2015.9.7.15 ISSN: 1738-9976 IJSIA Copyright 2015 SERSC Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study Areej Al Hogail Department of Information Systems College of Computing and Information Sciences King Saud University alhogail@ccis.imamu.edu.sa