The Human Factor of Cyber Crime and Cyber Security

Challenges: September 11th has marked an important turning point that exposed new types of security threats and disclosed how cyber criminals pursuit of their long-term strategic objectives that could result in not only large scale human casualties but also profound damage to national power and prestige. According to recent studies and reports[1], violent extremists are trying to obtain insider position that may increase the impact of any attack on the critical infrastructure and there is also a probability that any terrorist group attacks may cause the collapse of any major critical infrastructure organization's data. Based on these reports it is clear that their actions pose a significant threat that could potentially impact critical services, financial impact, people lives and even democracy. It is of utmost importance to adopt important measures in order to secure critical infrastructure and thus lower the level of threats while preserving the rights of citizens. States have an extreme interest in detecting malicious insiders and to counter human threats. Different agencies have invested billions of dollars in different technical measures for years now. Such as, access control implemented through passwords, authentication, biometric authentication and physical certification is recognizable as usernames and passwords pairs and firewalls, data leakage prevention and behavioral-pattern threat detection. However, various studies and researches demonstrate that security software devices are normally failed as these measures are normally designed to defend against external threats to secure critical infrastructure and do not protect against internal and external attacks aided by internal help in the organization.

The threat of malicious insider in the cyber-crime is very real. The aim of this research to create a single, actionable framework that engages all stakeholders to safeguard critical infrastructure from malicious exploits with a variety of specialized security solutions, various policies, threat management, management process, trainings and security awareness policies to mitigate these threats. An integrated security approach will also develop a comprehensive cyber terrorism strategy based on my research and professional experiences by taking appropriate steps to control access to sensitive data and to monitor malicious activities and to improve defenses on operating systems and networks.

Research Questions: 1) What are the existing security vulnerabilities, the methods of attacks and consequences, range of potential insider/outsider actions that could be exploited by human factors? 2) How to develop a security awareness culture to improve security decision making, which countermeasures and policies can be taken. 3) How do these policies and actions contribute to improving risk mitigation for insider threats in critical infrastructure?

[1] http://info.publicintelligence.net/DHS-InsiderThreat.pdf

Objectives: 1) To investigate the real nature and magnitude of the human factor problems by means of reviewing relevant information, security surveys, taking into consideration the incidents knowledge and the opinion of security experts, psychologists and stakeholders. 2) To understand the potential for psychological indicators of an insider becoming a threat. 3) To focus on advanced security strategies, frameworks, models, and assessment methods to analyze the root causes, related risks and identify countermeasures and presents recommendations that will assist agencies in measuring, mitigating and managing the insider threats. 4) To evaluate mitigation strategies through a layered defense strategy consisting of people, process, security awareness culture, guidelines, education, policy frameworks, and technology perspectives.

Study Design & Methodology:

1. **Human Factor Analysis (Month 01 - 02):** in the first phase, I will analyze the newest approaches to topics related to human factors involved in critical infrastructure security by means of reviewing relevant publications, security surveys, and taking into consideration the incidents knowledge in order to find the real nature and magnitude of the malicious insider.
2. **Human Factor Vulnerability Assessment (HVA) Framework (Month 02 - 04):** This framework will include interviews of security experts, psychologists and stakeholders, employees, security personnel, technical and non-technical staff, administrators, and different levels of organization management into a single and actionable assessment framework to assess organizational structure, its infrastructure, employee roles and responsibilities, actual events of human threats incidents.
3. **Analysis and Assessment (Month 04 - 05):** This phase will be developed based on the analysis reports defined in Task 1 and 2. It will analyze the key issues of concern with both technical and non-technical vulnerabilities to identify the best practices including individual and organizational actions and responses. Assessment reports will be generated on the basis of these reports, and a plan of action and security standards to increase the agencies' ability to prevent, detect and respond to human threats.
4. **Multi-Layered Security Strategy (Month 05 - 12):** This task will carry out a multi layered security strategy in four critical steps based on the security standards defined in Task 3. This phase will focus on trainings, programs, guidelines, security policies educations and awareness to understand the roles and responsibilities related to the organisational mission to protect critical infrastructure from human threats – for which they are responsible for. After the first release, evaluation of the security mechanisms will be developed to monitor compliance and effectiveness of this task to revise the specification and architecture according to the experimental results obtained at that time. These critical steps are:

4.1.1 Human Factor Security Awareness and Training Program Development

4.1.2 Security Awareness and Training Material Development

4.1.3 Security Program Implementation Consultancy

4.1.4 Post-Implementation Security Program Consultancy and Periodical Evaluation

4.1 Human Factor Security Awareness and Training Program Development (Month 05 - 06): This task will identify what awareness, training and education are needed to mitigate the human factors in organization (i.e., what is required)? How are these needs being addressed by agencies, where are the gaps between the needs, what is being done and what more needs to be done for gap analysis and targeting deficient areas for early rollout. Which needs are most critical in critical environment? The roles and responsibilities of organization's personnel will be identified in design and implementation to maintain security standards.

4.2 Security Awareness and Training Material Development (Month 06 - 07): This task will developed a standardized framework and material to identify what behavior we do want to reinforce and what skills we do want the organization's management and their employees to learn and apply to mitigate human threats. The topics I will cover in this task are: social engineering tricks, malicious insiders, shoulder surfing, dumpster diving, tailgating, access control issues, visitor control and physical access to spaces as well as handling incident response. A unified database will be built that will consist of incidents, case studies for malicious related activates, vulnerabilities, lessons learned, and physiological profiles or statistics regarding the insider and insider misuse, abuse or social engineering activities to develop recommendations for technology and policy solutions for future problems in critical environment. Lesson learned and psychological profiles will provide managers, security specialists and medical personnel a profile of the insider to enable them to identify potential abusers before they cause serious damage.

4.3 Security Program Implementation Consultancy (Month 07 - 09): This task will focus on the implementation of a multi layered strategy with 1) Training 2) Programs and 3) Education and awareness with techniques to deliver security program material. Training material will ensure that organizations are appropriately trained in how to face human factors in critical situations. It will be ensured that the awareness and training material is effectively deployed to not only reach the intended audience but to become also deeply ingrained in their everyday work. Training material will be developed in a way that it is reviewed periodically and updated when necessary as well as provide assistance in establishing a tracking and reporting strategy. Different activities will be established to evaluate on a continuing basis the effectiveness of available security methods and tools of all types to mitigate that risk. Methods and techniques will be developed regarding discarded storage media including USB sticks,

printouts and the like which may contain sensitive information, as well as classifying the sensitive information in data centers to enforce mandatory and discretionary access control mechanisms. Security programs will recommend best methods, guidelines and technologies dealing with human factor issues.

4.3.1 Techniques for Delivering Awareness Material (Month 09 - 10): Techniques will include, but will not be not limited to teleconferencing sessions, interactive video training, Web based training, videos, posters ("do and don't lists" or checklists), screensavers and warning banners/messages, instructor-led sessions as well as awards program, e.g., letters of appreciation.

4.4 Post-Implementation Security Program Consultancy and Periodical Evaluation (Month 10 - 12): Once the security program has been implemented, this task will carry out the necessary analysis, testing and evaluation of the security mechanisms developed to monitor compliance and effectiveness of the multi layered security strategy. Audit procedures will be in place to determine what will be audited, how behaviors will be analyzed, how results will be reported (such as confidential reports) and to whom, and average frequency of audits. A procedure will be carried out for randomly auditing employee system access to monitor malicious behavior. A feedback mechanism will be designed to address objectives initially established for the security program. This strategy will consist of evaluation forms, surveys, interviews, status reports, focus groups, independent observation, and bench marking etc.

Impact and Expected Benefits: The purpose of this research is to mitigate psychological, technical, organizational, and contextual factors I believe contribute to human sabotage against critical information and espionage and address behavioral issues that influence insider threat. It will identify existing security vulnerabilities and will facilitate more accurate risk assessments, includes low-cost, easily implemented policy solutions for critical agencies for long term effect. It proposes actionable framework, techniques and practices in order to ensure that such disruptions through human threats are infrequent, of minimal duration, manageable, and cause the least damage possible, thus it lower the level of terrorist threats and manage this risk to be below the predefined security level. The employed methodology will also suggest which countermeasures can be taken by organisations to protect themselves against human threats. The methodology will focus on multi layered security strategies, guidelines, frameworks, models, and assessment methods linked to the overall architecture of this project to analyze the root causes of these problems in order to improve security decision making and judgment in social engineering attacks and insider threats to secure critical infrastructure of the state.

References:

[1] Sahito, Farhan Hyder, and Wolfgang Slany. "Advanced Personnel Vetting Techniques in Critical Multi-Tennant Hosted Computing Environments." International Journal of Advanced Computer Science and Applications (IJACSA). Vol. 4, No.5, 2013..

[2] Sahito, Farhan Hyder, and Wolfgang Slany. "Functional Magnetic Resonance Imaging and the Challenge of Balancing Human Security with State Security." Human Security Perspectives 1 (European Training and Research Centre for Human Rights and Democracy (ETC), Graz, Austria) 2012 (1):38–66

[3] Warkentin, Merrill, and Robert Willison. "Behavioral and policy issues in information systems security: the insider threat." European Journal of Information Systems 18.2 (2009): 101.

[4] Colwill, Carl. "Human factors in information security: The insider threat–Who can you trust these days?." Information security technical report 14.4 (2009): 186-196.

[5] Cole, Eric, and Sandra Ring. Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft: Protecting the Enterprise from Sabotage, Spying, and Theft. Syngress, 2005.

[6] Senator, Ted E., et al. "Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity." (2013).

[7] Young, William T., et al. "Use of Domain Knowledge to Detect Insider Threats in Computer Activities." Workshop on Research for Insider Threat, IEEE CS Security and Privacy Workshops, San Francisco. 2013.

[8] Ted, E., et al. "Detecting insider threats in a real corporate database of computer usage activity." Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2013.

[9] Dodge Jr, Ronald C., Aaron J. Ferguson, and Dawn M. Cappelli. "Introduction to Insider Threat Modeling, Detection, and Mitigation Minitrack." System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE, 2013.

[10] Huth, Carly L. "The insider threat and employee privacy: An overview of recent case law." Computer Law & Security Review 29.4 (2013): 368-381.

Farhan Hyder Sahito (fsahito@ist.tugraz.at**)**

http://www.ist.tugraz.at/farhansahito.html

Tel +43-664-1275730 Mobile: +43-680-406-5176