MERIT *Interactive* Insider Threat Training Simulator

Carnegie Mellon University Software Engineering Institute CERT Program

Objective: An organization's risk due to insider cyber attacks depends on the complex interaction of the organization's business policies and procedures, organizational culture, and technology over time. In this project, we are developing a stand-alone tool that can be used for widespread training for managers on insider threat risk mitigation. We are using state of the art multi-media technologies to develop a training simulator (which we call MERIT *InterActive*, or MERIT$_{IA}$) that immerses users in a realistic business setting from which they make decisions regarding how to prevent, detect, and respond to insider actions and see the impacts of their decisions in terms of key performance metrics. In order to succeed in the simulation, the user must effectively balance:

- Requirements to meet project deadlines,
- Need for good management practices, such as spending "face time" with employees,
- Working with IT to implement proactive IT practices and policies,
- Working with management, human resources, and the IT department to respond to unplanned emergencies, such as network crashes or disgruntled employees.

If the above requirements are not balanced appropriately then the user "loses" by being the victim of an insider attack or being fired for poor performance. However, there are different degrees of "losing"; the damages and recovery efforts required as a result of their actions throughout the simulation can vary significantly. The interface is being designed to encourage users to run the simulation multiple times; they receive coaching on their performance at key "checkpoints" so that they learn from their mistakes and can improve their performance in the safety of a simulation environment.

Background: In collaboration with the U.S. Secret Service and the Department of Defense, the CERT Insider Threat Team has gathered and analyzed over 200 insider threat cases, including cases of IT sabotage, fraud, theft of sensitive or proprietary information, and espionage. The focus of the CERT team has been to approach all insider threat projects by building collaborative teams composed of both technical and psychological experts. MERIT$_{IA}$ is based on a System Dynamics simulation model that was developed during a series of group modeling sessions with representatives from the DoD, industry, and academia.

Broader implications: Broad application of MERIT$_{IA}$ will help organizations across the U.S and abroad to significantly reduce their risk and losses due to insider attacks. Application to better protect organizations that control U.S. critical infrastructures will benefit national security and the general public as a whole.

Technical approach: We are working jointly with a team at Carnegie Mellon University's Entertainment Technology Center (ETC) to develop a compelling multi-media training simulator. We are using an evolutionary prototyping development methodology that involves an iterative process of prototyping and requirements refinement. The current focus of the effort is on insider IT sabotage, but the engine is being designed to accommodate the ability to seamlessly "plug and play" additional scenarios.

Progress: We have developed a fictional case scenario that is representative of a preponderance of actual cases of insider IT sabotage that we have analyzed. The ETC team is on the second version of a user interface design that uses state of the art graphics, video, and audio technologies to bring the scenario to life. The evolving simulator based on the scenario and user interface provides a coherent, well-grounded, and engaging environment for teaching the primary lessons for mitigating the risk of insider IT sabotage.

A proof of concept will be completed by May 2007; we are currently seeking funding for development of a production version of the MERIT$_{IA}$ training simulator.

MERIT$_{IA}$ User Benefits: MERIT$_{IA}$ will help managers, information technology, and human resources better understand insider threat risks and the effects of decisions on the promotion or mitigation of that risk. The technology will empower organizations to develop comprehensive, efficient, and justifiable defenses to insider threats along with the organizational understanding and support needed to maintain a strong security posture over time.

For more information, please contact us at insider-threat-feedback@cert.org.