Management, Human Resources, and Information Technology: Working Together to Prevent and Detect Insider Threats Insider Threat Workshop

CERT® Program, Software Engineering Institute, Carnegie Mellon University

The CERT Program at Carnegie Mellon University's Software Engineering Institute has been researching insider threats since 2002. Our Insider Threat Study, conducted in partnership with the U.S. Secret Service, collected and analyzed over 150 actual insider threat cases that occurred between 1996 and 2002 and published a series of reports detailing findings and implications of the study. In addition to the initial 150 cases, we have gathered and analyzed approximately250 additional insider threat cases, from 2002 through the present, to supplement the original Insider Threat Study. Based on that research, Carnegie Mellon CyLab funded the MERIT[1] project, which produced the *Common Sense Guide to Prevention and Detection of Insider Threats*[2].

As part of MERIT we have developed models for three types of insider threats: IT sabotage, theft of intellectual property (e.g. trade secrets), and fraud. These models communicate the key technical, social, and organizational patterns of behavior observed in a majority of cases. The models help us to better understand and communicate how the threat evolves over time and effective mitigations of the risk. We have also created an insider threat vulnerability assessment. The assessment carefully evaluates the organization's defensive posture against malicious activity carried out by insiders in the cases we have reviewed. The assessment is a holistic process, which addresses technical, organizational, personnel, security, and process issues.

We have combined all of our work into a two day workshop on insider threat. The workshop consists of presentations and interactive exercises in which participants are led through portions of the insider threat assessment along with representative case studies. The purpose of the exercises is to assist participants in assessing their own organization's vulnerability to insider threat in specific areas of concern. Our goal is that participants leave the workshop with actionable steps that they can take to better manage the risk of insider threat in their organization.

The target audience for the workshop is managers and executives who have the authority to influence decision makers within their organization. We have worked with noted psychologists with extensive experience in insider threats, espionage, and electronic crimes for all of our insider threat projects, including psychologists from the Secret Service, FBI, and Department of Defense. Therefore, we address the entire problem space, including psychological, organizational culture, policy, procedure, and technical issues.

Day 1

Introduction

a. Purpose of the workshop
b. Introduction of workshop leader and participants
c. How bad is the insider threat?
d. Background on CERT's insider threat research

Module 1: Overview of Insider Threats

a. Discussion of types of insider crimes
    i. IT Sabotage
    ii. Theft of Intellectual Property (e.g. trade secrets)
    iii. Fraud
b. Case examples for each type of crime

Module 2: Insider IT Sabotage

a. Characteristics of the insiders and victim organizations
b. Behavioral and technical observations of the cases
c. Case Studies
d. MERIT Model of Insider IT Sabotage

Interactive Exercise 1: Insider IT Sabotage

a. Case examples
b. Discussion of issues from insider threat diagnostic

Best Practices for Prevention or Detection of Insider Threat (Part I)

Day 1 Wrap-Up

Day 2

Module 3: Insider Theft of Intellectual Property

a. Characteristics of the insiders and victim organizations
b. Dynamics of the incidents
c. Technical aspects
d. Impacts

Interactive Exercise 2: Insider Theft of Intellectual Property

a. Case examples
b. Discussion of issues from insider threat diagnostic

Module 4: Insider Fraud

a. Characteristics of the insiders and victim organizations
b. Dynamics of the crimes
c. Technical aspects
d. Impacts

Module 5: Insider Threat Detection Strategies

a. IT Sabotage
b. Demonstration – Detection of actual IT sabotage attack
c. Fraud
d. Theft of Intellectual Property
e. Demonstration – Detection of actual theft of intellectual property attack
f. Final Thoughts

Best Practices for Prevention or Detection of Insider Threat (Part II)

Day 2 Wrap Up

a. Future work planned by CERT
b. Feedback on the workshop by participants