



Insider Threat Vulnerability Assessment

CERT[®] Program, Software Engineering Institute, Carnegie Mellon University

Introduction

CERT's insider threat research focuses on both technical and behavioral aspects of actual compromises. We produce reports, training, models, and tools to raise awareness of the risks of insider threat and to help identify the factors influencing an insider's decision to act, the indicators and precursors of malicious acts, and the countermeasures that will improve the survivability and resiliency of the organization.

Insiders can be current or former employees, contractors, or business partners who have or had authorized access to their organization's system and networks. These individuals are familiar with internal policies, procedures, technology, and they can exploit that knowledge to facilitate attacks and even collude with external attackers. Our research, conducted since 2001, has focused on gathering data about actual malicious insider acts, including IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to our nation's critical infrastructures.

Our work has been well-received by industry and government, but we are regularly asked for an assessment instrument based on our research that evaluates how vulnerable an organization is to insider threat. Because the insider threat problem is so complex—involving physical security, information technology, management, data “owners,” software engineering, and human resources—organizations need assistance in merging the wealth of available guidance into a single actionable framework. To meet this need, we have developed an assessment that organizations can use to safeguard their critical infrastructure.¹

Approach

The insider threat vulnerability assessment enables organizations to gain a better understanding of insider threat and an enhanced ability to assess and manage associated risks. It merges technical, organizational, personnel, business security, and process issues into a single, actionable framework. The instrument is structured to encompass all stakeholders in the fight against insider threat.

The assessment instrument is based on more than 250 insider threat cases in our database. The instrument addresses technical, psychological, process, and policy issues, and it is structured

¹ The development of this assessment was funded by Carnegie Mellon University's CyLab.



around information technology, human resources, physical security, business processes, legal, management, and organizational issues.

The CERT project team will travel to your site to conduct an on-site assessment. The three-day assessment will consist of interviews with key organizational personnel. We will then give you a confidential report that contains the findings of the assessment and considerations for potential mitigation strategies. Organizations have used this report to

- identify and implement short-term tactical countermeasures
- help guide their ongoing risk management process for implementing long term, strategic countermeasures
- justify follow-up actions to key decision makers

CERT will sign non-disclosure agreements; and, as with all of our insider threat research, all collaborations will remain confidential.

Summary

We expect that the CERT insider threat vulnerability assessment, which is based on psychological expertise as well as technical expertise, will assist you to better safeguard your critical infrastructure. The purpose of the assessment is to

- enable you to gain a better understanding of your vulnerability to insider threat and an enhanced ability to assess and manage associated risks
- include technical, organizational, personnel, and business security and process issues from all of our past research in a single, actionable framework
- benefit all individuals involved in the insider threat vulnerability assessment process: information technology, human resources, physical security, data and business process “owners”, and all levels of organizational management

Our insider threat research has proven that the insider threat problem is quite complex, and organizations are in need of this type of instrument. It is critical that the assessment 1) encompass policies, practices and technologies; 2) be empirically based yet adaptable to current trends and technologies; and 3) focus on both prevention and detection strategies.