



Software Engineering Institute

Carnegie Mellon

Identifying Vulnerabilities and Issues of Concern

Understanding how susceptible you are to insider threat is a valuable step in developing a remediation strategy. Our assessment explores the entire organization, including technical vulnerabilities, business process gaps, management issues, and the ability to deal effectively with behavioral issues.



Insider Threat Vulnerability Assessment

Our Research Provides the Foundation

CERT® 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. With funding from Carnegie Mellon University's CyLab and the Department of Homeland Security, we have developed an assessment instrument that organizations can use to safeguard their critical infrastructure.

Organizations Gain Insights

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. The assessment instrument, which is based on more than 550 insider threat cases in our database, encompasses information technology, human resources, physical security, business processes, legal, management, and organizational issues. It merges technical, behavioral, process, and policy issues into a single, actionable framework.

For the assessment, members of the Insider Threat Center staff will spend three to five days at your organization. During that time, we will review documents, interview key personnel in your organization, and observe key processes and



For more information about our research, visit the CERT website:

www.cert.org/insider_threat

If you are interested in scheduling an assessment, email Insider Threat Center staff:

insider-threat-feedback@cert.org

Insider Threat Vulnerability Assessment (continued)

Organizations Gain Insights (continued)

security issues. We will sign non-disclosure agreements, and all collaborations will remain confidential.

After the on-site visit, we will provide you with 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

Consider Taking Advantage of This Valuable Instrument

Our research has proven that the insider threat problem is quite complex, and organizations need an instrument that has the following characteristics:

- encompasses policies, practices, and technologies
- is empirically based yet adaptable to current trends and technologies
- focuses on prevention, detection, and response strategies

The CERT insider threat vulnerability assessment, which is based on psychological expertise as well as technical expertise, will help 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