Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

U.S Department of Homeland Security

United States Secret Service

Press Release

SECRET SERVICE AND CERT® COORDINATION CENTER RELEASE COMPREHENSIVE REPORT ANALYZING INSIDER THREATS TO BANKING AND FINANCE SECTOR

First of a Series of Reports to Focus on Threats to Information Systems and Data in Critical Infrastructure Sectors

(Washington, DC) — The U.S. Secret Service, a part of the U.S. Department of Homeland Security, and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center (CERT/CC) today announced the findings of the first Insider Threat Study report, a collaborative effort to better understand insider activities affecting information systems and data in critical infrastructure sectors. This study, made possible by significant financial support from the Department of Homeland Security's Science and Technology Directorate, is the first of its kind to provide a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the threats.

The report released today focuses on the people who have had access to and have perpetrated harm using information systems in the banking and finance sector, which includes credit unions and financial institutions. The findings underscore the importance of organizations' technology, policies and procedures in securing their networks against insider threats, as most of the cases showcased in the report were perpetrated by insiders with minimal technical skills. Various proactive practices are among the suggestions offered by the report.

"With the potential for cyber crime and network intrusion expanding rapidly around the globe, the importance of cooperation with our partners in the private sector is greater than ever," said Secret Service Director W. Ralph Basham. "The Insider Threat Study is a solid example of the role the Secret Service and its partners can play in understanding threats and helping to prevent serious crimes such as network intrusions, identity theft and financial fraud."

"This study provides concrete insight into the insider threat problem. It also demonstrates the value that can be gained when organizations are willing to share their data and experiences with

others," said Richard D. Pethia, Director of CERT/CC. "I applaud the organizations that participated in this study and encourage others to share their experiences so that we can all deal more effectively with the growing cyber security problem."

"At a time when our national security is more closely linked than ever to the protection of our nation's electronic and financial infrastructure, the Insider Threat Study serves as a crucial reminder for all of us to protect sensitive information by closely monitoring and safeguarding network usage each and every day and reporting suspected intrusions" said Undersecretary Charles McQueary, Ph.D., the Department of Homeland Security, Science and Technology Directorate.

Major Findings of the Insider Threat Study Report on the Banking and Finance Sector

This first report from the Insider Threat Study offers important insight for law enforcement officials, corporate security professionals, human resource personnel, and others responsible for the protection of an organization's systems and data. Twenty-three cases, carried out by 26 insiders between 1996 and 2002, were examined in the banking and finance sector. Major findings, which present examples of insider methods as well as means of detecting insider activities in this sector, include:

- Most of the incidents in the banking and finance sector were not technically sophisticated or complex. They typically involved the exploitation of non-technical vulnerabilities such as business rules or organization policies (rather than vulnerabilities in an information system or network) by individuals who had little or no technical expertise. In 87% of the cases the insiders employed simple, legitimate user commands to carry out the incidents, and in 78% of the incidents, the insiders were authorized users with active computer accounts.
- The majority of the incidents (81%) were devised and planned in advance. Furthermore, in most cases, others had knowledge of the insider's intentions, plans, and/or activities. Those who knew were often directly involved in the planning or stood to benefit from the activity.
- Most insiders (81%) were motivated by financial gain, rather than a desire to harm the company or information system.
- Insiders in this report fit no common profile. Only 23% held a technical position, 13% had a demonstrated interest in "hacking" and 27% had come to the attention of a supervisor or co-worker prior to the incident.
- Insider incidents were detected by internal, as well as external, individuals – including customers.
- The impact of nearly all insider incidents in the banking and finance sector was financial loss for the victim organization: in 30% of the cases the financial loss exceeded $500,000. Many victim organizations incurred harm to multiple aspects of the organization.
- Most of the incidents (83%) were executed physically from within the insider's organization and took place during normal business hours.

About the Insider Threat Study

The Insider Threat Study is one component of an ongoing partnership between the Secret Service's National Threat Assessment Center (NTAC) and the Software Engineering Institute's CERT Coordination Center, , designed to develop information to help private industry, government, and law enforcement better understand, detect and ultimately prevent harmful insider activity.

The definition of an insider for this study includes current, former, or contract employees of an organization. The cases analyzed in the Insider Threat Study involve incidents in which an insider intentionally exceeded or misused an authorized level of system access in a manner that affected the organization's data, daily business operations, or system security, or involved other harm perpetrated via a computer.

For the Insider Threat Study, researchers from the Secret Service CERT/CC have focused on identifying the physical and online behaviors and communications that insiders engaged in before the incidents, as well as how the incidents were eventually executed, detected, and the insider identified. This approach addresses a broader phenomenon than previous studies on the topic of insider activity.

This report and other information from the Insider Threat Study will be made available throughout the private sector and federal, state and local governments to assist in the prevention of harmful insider incidents. In addition to the report released today on the banking and finance sector, the Secret Service and CERT/CC will release additional reports in the coming months that focus on other critical infrastructure sectors.

Since 2001, the Secret Service and the CERT/CC have collaborated on the Critical Systems Protection Initiative – or CSPI – which includes multiple efforts to identify, assess, and manage potential threats to and vulnerabilities of critical systems. The collaboration represents an effort to augment current security and protective measures through two components:

- Finding ways to identify, assess, and mitigate cyber security threats to critical systems and data that impact physical security or that threaten the mission of the organization
- Finding ways to identify, assess, and manage individuals who may pose a threat of compromise to those critical systems and data.

At the direction of Undersecretary Charles McQueary, Ph.D., the Department of Homeland Security's Science and Technology Directorate provided substantial funding for the Insider Threat Study in both FY03 and FY04, which was critical to ensuring the completion of the study and dissemination of findings.

About the United States Secret Service

The Secret Service was originally founded in 1865 for the purpose of suppressing the counterfeiting of U.S. currency. Since that time, it has grown into one of the premier law enforcement organizations charged with investigating financial crimes, as well as the protection of the nation's

leaders, visiting foreign dignitaries and events of national significance. The Secret Service has taken a lead role in the developing area of cyber crime, establishing working partnerships in both the law enforcement and business communities to address such issues as protection of critical infrastructure, internet intrusions and associated fraud.

The Secret Service investigates a wide array of criminal misuses of electronic technology, from unauthorized computer access to credit card fraud, to cellular and land line telephone service tampering, the production of false identification, counterfeit currency, threats made against the President, narcotics, illegal firearms trafficking and even homicides.

The National Threat Assessment Center was created by the Secret Service in 2000 to provide leadership and guidance to the emerging field of threat assessment. Two previous NTAC studies, the Exceptional Case Study Project and the Safe School Initiative, analyzed physical attacks on public officials and public figures and attacks on schools. Both studies focused on identifying information that was operationally relevant and that could help prevent future violent or disruptive incidents. Findings from the Insider Threat Study may similarly enhance efforts within law enforcement, corporate security, and others in prevention, early detection, and investigation of cyber-related crimes.

About CERT® Coordination Center

The CERT® Coordination Center is located at Carnegie Mellon University's Software Engineering Institute in Pittsburgh, Pennsylvania. The Software Engineering Institute is a Department of Defense-sponsored federally funded research and development center. The CERT/CC was established in 1988 to deal with security issues on the internet. It now partners with and supports the Department of Homeland Security's National Cyber Security Division and its US-CERT to coordinate responses to security compromises, identify trends in intruder activity, identify solutions to security problems and disseminate information to the broad community. The CERT/CC also conducts research to develop solutions to security problems and provides training to help individuals build skills in dealing with cyber security issues.

###

EDITOR'S NOTE: The complete first report from the Insider Threat Study can be found at http://www.secretservice.gov/ntac.shtml and http://www.cert.org/archive/pdf/bankfin040820.pdf.

For questions concerning this release, please contact the United States Secret Service Office of Government and Public Affairs at 202-406-5708 or Kelly Kimberland at the CERT® Coordination Center at 412-268-4793.