FOR IMMEDIATE RELEASE

2005 E-CRIME WATCH™ SURVEY SHOWS E-CRIME FIGHTERS MAKING HEADWAY

Average Company Loss Estimated at More Than Half Million Dollars

Framingham, MA—May 3, 2005—Results from the 2005 E-Crime Watch survey, conducted among security executives and law enforcement personnel, by *CSO* magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, reveals the fight against electronic crimes (e-crimes) may be paying off. Thirteen percent (13%) of the 819 survey respondents—more than double the 6% from the 2004 survey—report the total number of e-crimes (and network, system or data intrusions) decreased from the previous year; 35% report an increase in e-crimes and 30% report no change. Almost one third (32%) of respondents experienced fewer than 10 e-crimes (versus the 25% reported in 2004), while the average number of e-crimes per respondent decreased to 86 (significantly less than 136 average reported in the 2004 survey). Respondents report an average loss of $506,670 per organization due to e-crimes and a sum total loss of $150 million.[1]

E-Crimes Impact

While the average number of e-crimes decreased year over year from 2003 to 2004, 68% of respondents report at least one e-crime or intrusion committed against their organization in 2004 and 88% anticipate an increase in e-crime during 2005. More than half (53%) expect monetary losses to increase or remain the same.

When asked what e-crimes were committed against their organizations in 2004, respondents cite virus or other malicious code as most prevalent (82%), with spyware (61%), phishing (57%) and illegal generation of spam email (48%) falling close behind. Phishing, a precursor to fraud and/or identity theft, jumps from 31% in the 2004 survey to 57%, the largest single percent increase of an e-crime year over year.

Of those who experienced e-crimes, more than half of respondents (55%) report operational losses, 28% state financial losses and 12% declare harm to reputation as a result. Interestingly, one third (31%) of respondents do not have a formal process or system in place for tracking e-crime attempts, and 39% do not have a formalized plan outlining policies and procedures for reporting and responding to e-crimes, demonstrating room for improvement.

"Security practitioners are faced with new e-crimes on a daily basis. Phishing is a perfect example of a crime that entered the market and has just exploded," says Bob Bragdon, Publisher of *CSO* magazine. "It's not enough to just track these crimes. Businesses need to be doing a better job of formalizing their reporting procedures so law enforcement can help them combat the attacks and, over the long haul, minimize the threats."

Identifying, Monitoring & Reporting

Organizations, in both the public and private sectors, appear to be doing a better job identifying criminals. Only 19% of respondents experiencing e-crimes or intrusions in 2004 do not know whether insiders or outsiders were the cause, down from 30% in last year's survey. Respondents who identify the culprit indicate that 80% of the attacks come from outsiders and 20% from insiders (a drop from 29% in the 2004 survey).

Eighty percent (80%) of respondents report their organizations monitor their computer systems or networks for misuse and abuse by employees or contractors. Sixty-nine percent (69%) require internal reporting of misuse or abuse of computer access by employees or contractors. However, there is still an opportunity to progress in reporting e-crimes to outside officials. Among organizations experiencing e-crimes, the majority of respondents (78%) report that one or more cases were handled internally without involving legal action or law enforcement. The

[1] Monetary loss data not comparable to 2004 figures due to change in question format implemented to collect more precise data.

top three reasons stated for not referring an intrusion for legal action are: damage level insufficient to warrant prosecution (59%), lack of evidence/not enough information to prosecute (50%) and concerns about negative publicity (15%). However, only 31% of respondents consider themselves extremely or very knowledgeable in understanding U.S. laws about computer crimes; only 7% consider themselves knowledgeable about international laws.

"What is important for our partners in the private sector to know is that when an intrusion is not reported to law enforcement, that only enables the criminals to continue to do more—and possibly greater—damage elsewhere, " said Larry Johnson, Special Agent in Charge, Criminal Investigative Division, United States Secret Service. "The Secret Service philosophy is one of prevention. Together with our private industry partners, we have a proven track record of aggressively investigating and preventing electronic crimes that could adversely affect the businesses and citizens of this country."

Effective Practices

The top technologies used to combat e-crime are firewalls and automated virus scanning used by 99% of respondents, followed by physical security systems (94%), spyware/adware detection software (93%), intrusion detection systems (91%) and manual patch management (90%). For the second year in a row, manual patch management, a common strategy in use, is rated by respondents as the single least effective technology (26%). Among the most effective technologies, the use of firewalls is listed as most effective at 68%, followed by automated virus scanning (66%), encryption (58%), two-factor authentication (56%) and intrusion detection systems (50%). Moreover, the top five security policies and procedures in use by respondents to prevent or reduce an e-crime are: account/password management policies (74%), formal “inappropriate use” policy (71%), employee education and awareness programs (67%), monitoring of internet connections (65%) and corporate security policy (62%).

"The respondents rated employee security training, education and awareness programs, and regular communication as the most effective strategies for deterring insider threats. These strategies create a culture of security in the organization, where all employees understand that security is a shared responsibility,” said Dawn Cappelli, senior member of the technical staff with the Software Engineering Institute’s Networked Systems Survivability program.

About the 2005 E-Crime Watch Survey

The 2005 E-Crime Watch survey was conducted by *CSO* magazine in cooperation with the United States Secret Service and the CERT Coordination Center. The research was conducted to unearth e-crime fighting trends and techniques, including best practices and emerging trends. Respondent answers are based on the 2004 calendar year.

For the purpose of this survey, an electronic crime is defined as: any criminal violation in which a computer or electronic media is used in the commission of that crime. An intrusion is defined as: a specific incident or event perpetrated via computer that targeted or affected an organization’s data, systems, reputation or involved other criminal behavior. An insider is defined as: a current or former employee or contractor. An outsider is defined as: non-employee or non-contractor. The online survey of *CSO* magazine subscribers and members of the United States Secret Service’s Electronic Crimes Task Force members was conducted from March 3 to March 14, 2005. Results are based on 819 completed surveys. At a 95% confidence level, the margin of error is +/- 3.4%.

In addition to the 2005 E-Crime Watch survey team, the following security practitioners served as advisors to the project:

- Michael Assante, Vice President and Chief Security Officer, American Electric Power
- Bill Boni, Vice President and Chief Information Security Officer, Motorola
- Don Masters, Assistant Special Agent in Charge, Los Angeles Field Office, United States Secret Service

About CSO

Launched in 2002, *CSO* magazine provide chief security officers (CSOs) with analysis and insight on security trends and a keen understanding of how to develop successful strategies to secure all business assets—from people to information and financial value to physical infrastructure. The CSO portfolio includes its companion website (www.CSOonline.com), the CSO Perspectives™ conference and the CSO Executive Council™. The magazine is read by 27,000 security leaders from the private and public sectors. The U.S. edition of the magazine and website are the recipients of 50 awards to date, including the American Society of Business Publication Editor’s Magazine of the Year award as well as eight Jesse H. Neal National Business Journalism Awards and Grand Neal runner-up honors two years in a row. Licensed editions of CSO magazine are published in Australia, France and

Sweden. The CSO Perspectives™ conference, the first face-to-face conference designed for CSOs and featuring speakers from the national stage and the CSO community, offers educational and networking opportunities for pre-qualified corporate and government security executives. The CSO Executive Council is a professional organization of CSOs created to advance strategic security practices. *CSO* magazine, CSOonline.com, CSO Perspectives conference and the CSO Executive Council are produced by International Data Group's award-winning business unit: CXO Media Inc.

About CERT
The CERT® Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute in Pittsburgh, Pennsylvania, U.S.A. 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 R&D to develop solutions to security problems and provides training to help individuals build skills in dealing with cyber-security issues.

About the Secret Service's Electronic Crimes Task Forces (ECTF)
The USA PATRIOT ACT OF 2001 (HR 3162, 107th Congress, First Session, October 26, 2001, Public Law 107-56) ordered the Director of the United States Secret Service to take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States for the purpose of preventing, detecting and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

The ECTF mission is to establish a strategic alliance of federal, state and local law enforcement agencies, private sector technical experts, prosecutors, academic institutions and private industry in order to confront and suppress technology-based criminal activity that endangers the integrity of the nation's financial payments systems and poses threats against the nation's critical infrastructure. The ECTF model is built on trust and confidentiality without regulators or other outside influences. ECTF law enforcement members develop personal pre-incident relationships with corporate and academic ECTF members and are educated in business concepts such as risk management, return on investment and business continuity plans. As trained first responders to various forms of electronic crimes, ECTF law enforcement members approach incidents with the focus on business designs and information sharing with known corporate and academic individuals. Currently, 15 ECTF models are proving successful in Atlanta, GA; Boston, MA; Charlotte, NC; Chicago, IL; Cleveland, OH; Columbia, SC; Dallas, TX; Houston, TX; Las Vegas, NV; Los Angeles, CA; Miami, FL; New York, NY; Philadelphia, PA; San Francisco, CA; Washington, DC.

NOTE TO EDITORS: Findings from the 2005 E-Crime Watch survey can be found at http://www.csoonline.com/info/ecrimesurvey05.html. If you report any of the data from the 2005 E-Crime Watch survey, the data must be sourced as originating from: *CSO* magazine/U.S. Secret Service/CERT Coordination Center.

CONTACTS:

CSO magazine	CERT Coordination Center	U.S. Secret Service
Lori Piscatelli Scanlon	Kelly Kimberland	Jonathan Cherry
508.988.6838	412.268.8467	202.406.5708

###