

**Mar 12,2001**

**FOR IMMEDIATE RELEASE**

**Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar**

SAN FRANCISCO — The Computer Security Institute (CSI) announced today the results of its sixth annual "Computer Crime and Security Survey."

The "Computer Crime and Security Survey" is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States.

Based on responses from 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2001 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

Highlights of the "2001 Computer Crime and Security Survey" include:

Eighty-five percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.

Sixty-four percent acknowledged financial losses due to computer breaches.

Thirty-five percent (186 respondents) were willing and/or able to quantify their financial losses. These 186 respondents reported \$377,828,700 in financial losses. (In contrast, the losses from 249 respondents in 2000 totaled only \$265,589,940. The average annual total over the three years prior to 2000 was \$120,240,180.)

As in previous years, the most serious financial losses occurred through theft of proprietary information (34 respondents reported \$151,230,100) and financial fraud (21 respondents reported \$92,935,500).

For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001.

Thirty-six percent of respondents reported the intrusions to law enforcement; a significant increase from 2000, when only 25% reported them. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

Respondents detected a wide range of attacks and abuses. Here are some examples of attacks and abuses on the rise:

Forty percent of respondents detected system penetration from the outside (only 25% reported system penetration in 2000).

Thirty-eight percent of respondents detected denial of service attacks (only 27% reported denial of service in 2000).

Ninety-one percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems). Only 79% detected net abuse in 2000.

Ninety-four percent detected computer viruses (only 85% detected them in 2000).

For the third year, we asked some questions about electronic commerce over the Internet. Here are some of the results:

Ninety-seven percent of respondents have WWW sites.

Forty-seven percent conduct electronic commerce on their sites.

Twenty-three percent suffered unauthorized access or misuse within the last twelve months. Twenty-seven percent said that they didn't know if there had been unauthorized access or misuse.

Twenty-one percent of those acknowledging attacks reported from two to five incidents. Fifty-eight percent reported ten or more incidents.

Ninety percent of those attacked reported vandalism (only 64% in 2000).

Seventy-eight percent reported denial of service (only 60% in 2000).

Thirteen percent reported theft of transaction information (only 8% in 2000).

Eight percent reported financial fraud (only 3% in 2000).

Patrice Rapalus, CSI Director, remarks that the "Computer Crime and Security Survey," now in its sixth year, has served as a reality check for industry and government:

"Each year, the influence and impact of the CSI/FBI Computer Crime and Security Survey grows. It is an invaluable tool for information security practitioners in corporations and government agencies struggling to get the attention of their CEOs, CIOs and CFOs as well as for law enforcement officials working to make the case for closer cooperation with the private sector to stave off a cyber crime wave. The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprise-wide information security."

Bruce J. Gebhardt is in charge of the FBI's Northern California office. Based in San Francisco, his division covers fifteen counties, including the continually expanding Silicon Valley area. Computer crime is one of his biggest challenges.

" The results of this year's survey again demonstrate the seriousness and complexity of computer crime. The dynamic vulnerabilities associated with conducting business on-line remain a law enforcement challenge. In an effort to address this challenge the FBI and private sector have joined forces in an information sharing initiative named 'InfraGard.' For more information about InfraGard, please contact your local FBI office or visit the InfraGard website at [www.infagard.net](http://www.infagard.net)."

---

CSI, established in 1974, is a San Francisco-based association of information security professionals. It has thousands of members worldwide and provides a wide variety of information and education programs to assist practitioners in protecting the information assets of corporations and governmental organizations.

The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established the National Infrastructure Protection Center (NIPC) located at FBI headquarters and the Regional Computer Intrusion Squads located in selected offices throughout the United States. The NIPC, a joint partnership among federal agencies and private industry, is designed to serve as the government's lead mechanism for preventing and responding to cyber attacks on the nation's infrastructures. (These infrastructures include telecommunications, energy, transportation, banking and finance, emergency services and government operations). The mission of Regional Computer Intrusion Squads is to investigate violations of Computer Fraud and Abuse Act (Title 8, Section 1030), including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes.