U.S. Department of Justice

Federal Bureau of Investigation
2500 East T.C. Jester
Houston, TX 77008

Press Release January 19, 2006

NEW FBI COMPUTER CRIME SURVEY

The FBI is releasing a new Computer Crime Survey, the largest survey on these issues to date. The survey—developed and analyzed with the help of leading public and private authorities on cyber security—is based on responses from a cross-section of more than 2,000 public and private organizations in four states, including Iowa, Nebraska, New York and Texas. The survey can be viewed on the FBI website, www.fbi.gov.

The 2005 FBI Computer Crime Survey addresses one of the highest priorities in the Federal Bureau of Investigation. The purpose of the survey was to gain an accurate understanding of what computer security incidents are being experienced by the full spectrum of organizations within the United States.

Among the key findings:

* **Frequency of attacks.** Nearly nine out of 10 organizations experienced computer security incidents in a year's time; 20% of them indicated they had experienced 20 or more attacks.

* **Types of attacks.** Viruses (83.7%) and spyware (79.5%) headed the list. More than one in five organizations said they experienced port scans and network or data sabotage.

* **Financial impact.** Over 64% of the respondents incurred a loss. Viruses and worms cost the most, accounting for $12 million of the $32 million in total losses.

* **Sources of the attacks.** They came from 36 different countries. The U.S. (26.1%) and China (23.9%) were the source of over half of the intrusion attempts, though masking technologies make it difficult to get an accurate reading.

* **Defenses.** Most said they installed new security updates and software following incidents, but advanced security techniques such as biometrics (4%) and smart cards (7%) were used infrequently. In addition, 44% reported intrusions from within their own organizations, suggesting the need for strong internal controls.

* **Reporting.** Just 9% said they reported incidents to law enforcement, believing the infractions were not illegal or that there was little law enforcement could or would do. Of those reporting, however, 91% were satisfied with law enforcement's response. And 81% said they'd report future incidents to the FBI or other law enforcement agencies. Many also said they were unaware of InfraGard, a joint FBI/private sector initiative that battles computer crimes and other threats

through information sharing.

Bruce Verduyn—a special agent in Houston's Cyber Squad, which administered the survey-said this new survey differs from the annual CSI/FBI Computer Crime and Security Survey conducted by the Computer Security Institute and the FBI. "We surveyed about three times as many organizations and focused more on new technologies, where attacks originated, and how organizations responded," he said.

Agent Verduyn believes the survey is a clear sign of the urgent need for vigilance against both internal and external cyber assaults. Frank Abagnale, security consultant and subject of the movie "Catch Me If You Can," echoed those comments, saying: "Every company, both large and small, should study this survey and use the data as the basis for making changes. Those who ignore it do so at their peril."

Press Releases | Houston Homepage