ELEVENTH ANNUAL

2006

CSI/FBI

COMPUTER CRIME AND SECURITY SURVEY

GoCSI.com

2006

CSI/FBI

COMPUTER CRIME AND SECURITY SURVEY

by Lawrence A. Gordon, Martin P. Loeb,
William Lucyshyn and Robert Richardson

The Computer Crime and Security Survey is conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The survey is now in its 11th year and is, we believe, the longest-running continuous survey in the information security field. This year's survey results are based on the responses of 616 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities.

The 2006 survey addresses the major issues considered in earlier CSI/FBI surveys, thus allowing us to analyze important computer security trends. The long-term trends considered include:

- ❑ Unauthorized use of computer systems;
- ❑ The number of incidents from outside, as well as inside, an organization;
- ❑ Types of attacks or misuse detected, and;
- ❑ Actions taken in response to computer intrusions.

This year's survey also addresses several emerging security issues that were first probed only with the 2004 CSI/FBI survey. All of the following issues relate to the economic decisions organizations make regarding computer security and the way they manage the risk associated with security breaches:

- ❑ Techniques organizations use to evaluate the performance of their computer security investments;
- ❑ Security training needs of organizations;
- ❑ Organizational spending on security investments;
- ❑ The impact of outsourcing on computer security activities;
- ❑ The use of security audits and external insurance;
- ❑ The role of the Sarbanes–Oxley Act of 2002 on security activities, and;
- ❑ The portion of the information technology (IT) budget organizations devote to computer security.

This year's questionnaire also included some questions being introduced for the first time. In particular, an open-ended question about the current concerns of respondents has provided insight into the relative perceived urgency of concerns about issues such as data protection and instant messaging.

KEY FINDINGS

Some of the key findings from the participants in this year's survey are summarized below:

- Virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74 percent of financial losses.

- Unauthorized use of computer systems slightly decreased this year, according to respondents.

- The total dollar amount of financial losses resulting from security breaches had a substantial decrease this year, according to respondents. Although a large part of this drop was due to a decrease in the number of respondents able and willing to provide estimates of losses, the average amount of financial losses per respondent also decreased substantially this year.

- Despite talk of increasing outsourcing, the survey results related to outsourcing are similar to those reported in the last two years and indicate very little outsourcing of information security activities. In fact, 61 percent of the respondents indicated that their organizations do not outsource any computer security functions. Among those organizations that do outsource some computer security activities, the percentage of security activities outsourced is rather low.

- Use of cyber insurance remains low, but may be on the rise.

- The percentage of organizations reporting computer intrusions to law enforcement has reversed its multi-year decline, standing at 25 percent as compared with 20 percent in the previous two years. However, negative publicity from reporting intrusions to law enforcement is still a major concern for most organizations.

- Most organizations conduct some form of economic evaluation of their security expenditures, with 42 percent using Return on Investment (ROI), 21 percent using Internal Rate of Return (IRR), and 19 percent using Net Present Value (NPV). These percentages are all up from last year's reported numbers. Moreover, in open-ended comments, respondents frequently identified economic and management issues such as capital budgeting and risk management as among the most critical security issues they face.

- Over 80 percent of the organizations conduct security audits.

- The impact of the Sarbanes–Oxley Act on information security continues to be substantial. In fact, in open-ended comments, respondents noted that regulatory compliance related to information security is among the most critical security issues they face.

- Once again, the vast majority of the organizations view security awareness training as important. In fact, there is a substantial increase in the respondents' perception of the importance of security awareness training. On average, respondents from most sectors do not believe their organization invests enough in this area.