KEY FINDINGS

Some of the key findings from the participants in this year's survey are summarized here. The findings discussed below emphasize changes taking place in the computer security arena, as well as items not considered in previous CSI/FBI surveys.

- ❒ Unauthorized use of computer systems is on the decline, as is the reported dollar amount of annual financial losses resulting from security breaches.
- ❒ In a shift from previous years, both virus attacks and denial of service outpaced the former top cost, theft of proprietary information. Virus costs jumped to $55 million.
- ❒ The percentage of organizations reporting computer intrusions to law enforcement over the last year is on the decline. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity.
- ❒ Most organizations conduct some form of economic evaluation of their security expenditures, with 55 percent using Return on Investment (ROI), 28 percent using Internal Rate of Return (IRR), and 25 percent using Net Present Value (NPV).
- ❒ Over 80 percent of the organizations conduct security audits.
- ❒ The majority of organizations do not outsource computer security activities. Among those organizations that do outsource some computer security activities, the percentage of security activities outsourced is quite low.
- ❒ The Sarbanes-Oxley Act is beginning to have an impact on information security in some industries.
- ❒ The vast majority of the organizations view security awareness training as important, although (on average) respondents from all sectors do not believe their organization invests enough in this area.