NINTH ANNUAL

2004

CSI/FBI

COMPUTER CRIME AND SECURITY SURVEY

GoCSI.com

2004 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 CSI with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The survey is now in its ninth year and is, we believe, the longest-running survey in the information security field. This year's survey results are based on the responses of 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities.

The 2004 survey addresses the major issues considered in earlier CSI/FBI surveys, thus allowing us to analyze important computer security trends. In addition, this year's survey also addresses several new emerging security issues that have not been considered in previous CSI/FBI surveys. The new issues assessed in this year's survey include:

(1) the way organizations evaluate the performance of their investments in computer security
(2) the portion of the IT budget organizations devote to computer security
(3) the security training needs of organizations
(4) the level of organizational spending on security investments
(5) the impact of outsourcing on computer security activities
(6) the role of the Sarbanes-Oxley Act of 2002 on security activities
(7) the use of security audits and external insurance.

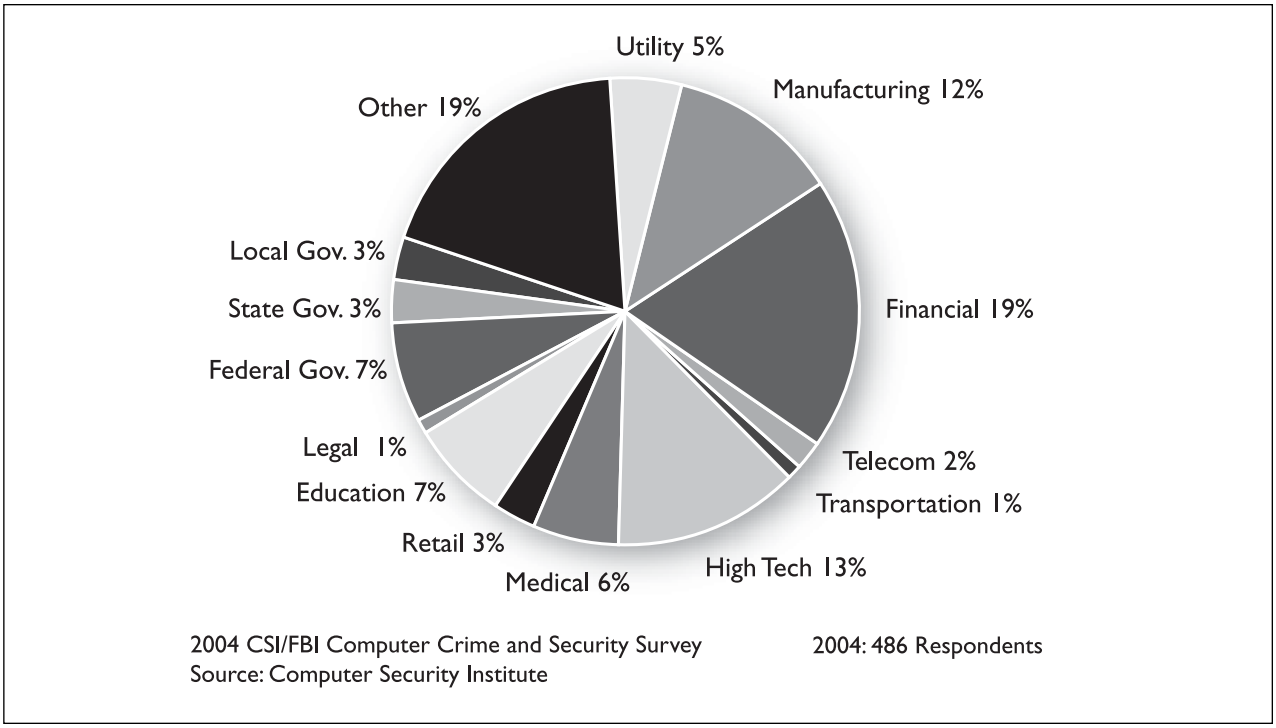
One way or the other, all of the new issues considered in this year's survey relate to the economic decisions that organizations make regarding computer security and the way they manage the risk associated with security breaches.[1]

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, the most expensive computer crime over the past year was due to denial of service.
- ❒ 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.

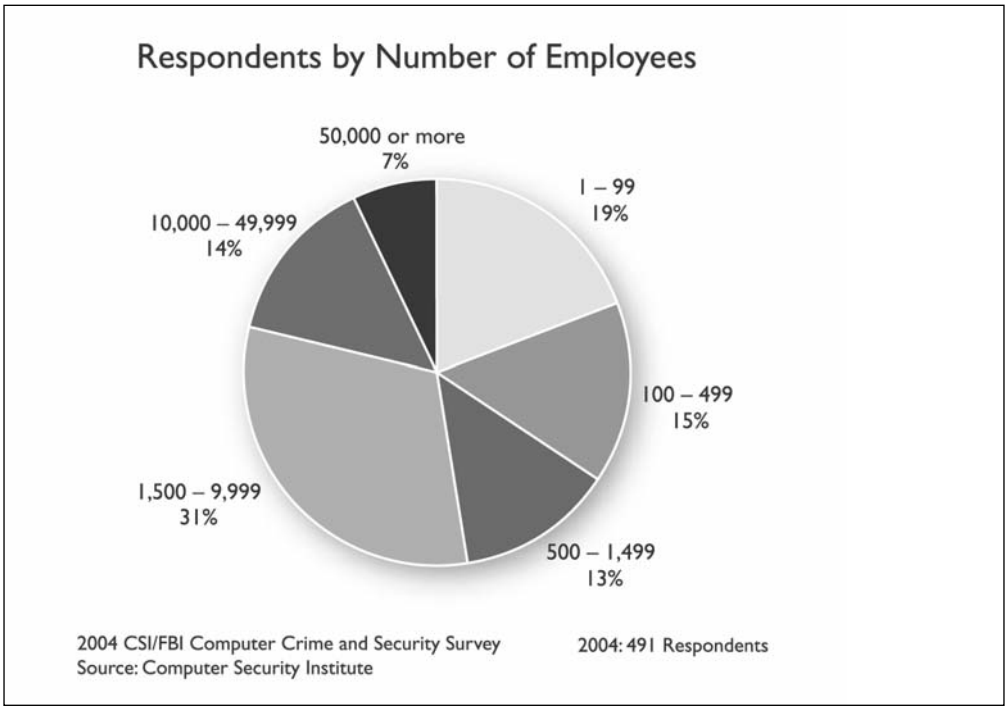
Figure 1. **Respondents by Industry Sector**



DETAILED SURVEY RESULTS

NOTE: The dates on the figures refer to the year of the report; the supporting data is based on the preceding year.

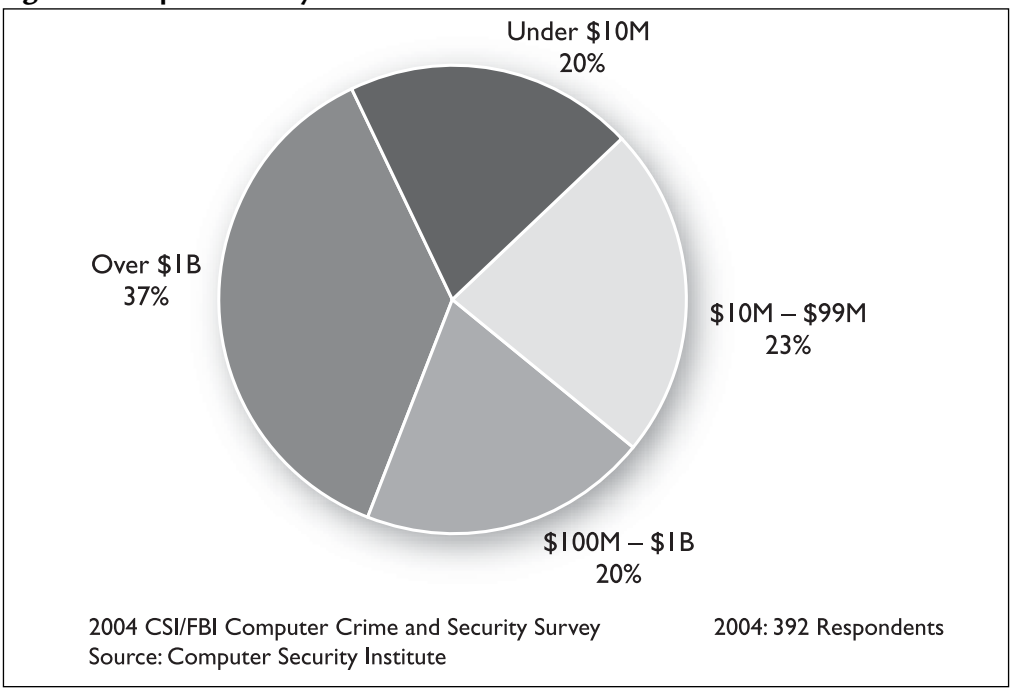
Figure 2. **Respondents by Number of Employees**



ABOUT THE RESPONDENTS

Information on the organizations and the individuals representing those organizations that responded to this year's survey are summarized in figures 1–4. As figure 1 shows, organizations participating in the survey cover many areas of both private and public sectors. The largest portion of responses came from the financial sector (19 percent), followed by high-tech (13 percent) and manufacturing (12 percent). The portion coming from government agencies (combining federal, state and local levels) was 13 percent, and educational institutions accounted for 7 percent of the responses. The diversity of organizations responding was also

Figure 3. **Respondents by Revenue**



reflected in the large portion (19 percent) designated as "Other."

The size of the organizations that are represented in the survey—as measured by number of employees—can be seen in figure 2. Organizations with 1,500 or more employees accounted for over half of the responses. The single largest size category of organizations responding was the category having from 1,500 to 9,999 employees. This category accounted for 31 percent of all responses. The category covering the biggest of the organizations, those with 50,000 or more employees, made up 7 percent of all responses. While large firms this year again accounted for most of the responses, it is noteworthy that a substantial portion of responses, 19 percent, came from firms having fewer than 100 employees.

Figure 3 shows the composition of the responding commercial enterprises by the annual revenue they generated. Since 57 percent of the firms responding generated annual revenues in excess of $100M, including 37 percent generating annual revenues in excess of $1B, the largest firms in America are well represented. Nevertheless, 20 percent of the responding firms generated annual revenues under $10M.

New to this year's survey is a categorization of respondents by job title. Figure 4 illustrates that 18 percent of the respondents were senior executives with the titles of chief executive officer (4 percent), chief information officer (8 percent) or chief security officer (6 percent). The majority (53 percent) of respondents had job titles of security officer, security manager or security director. An additional 9 percent of respondents had

Figure 4. **Respondents by Job Description**

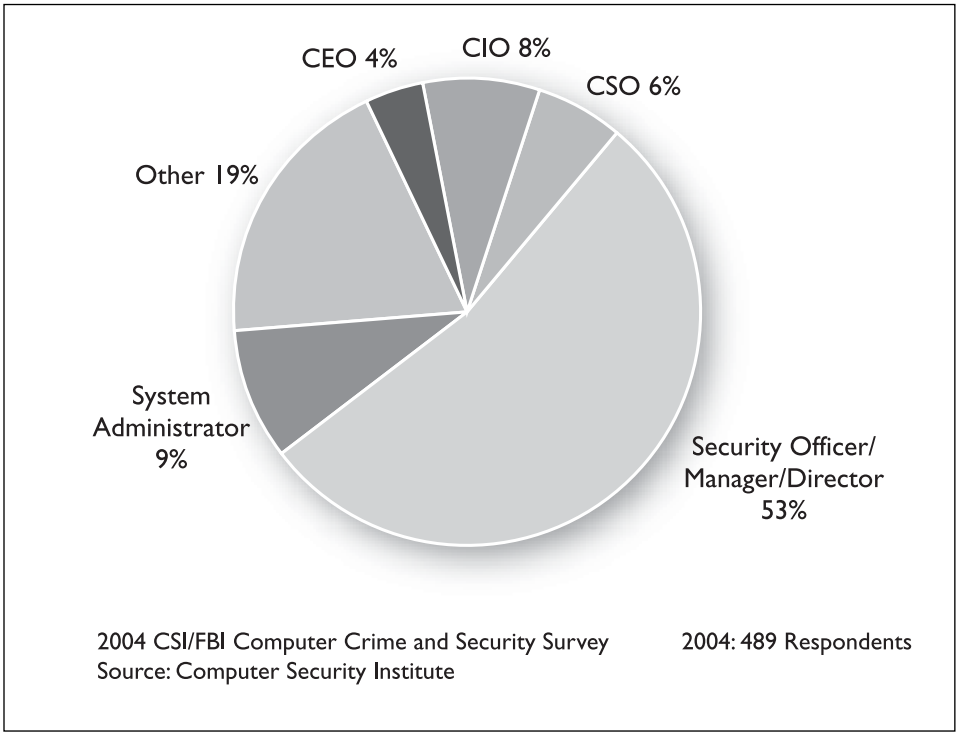
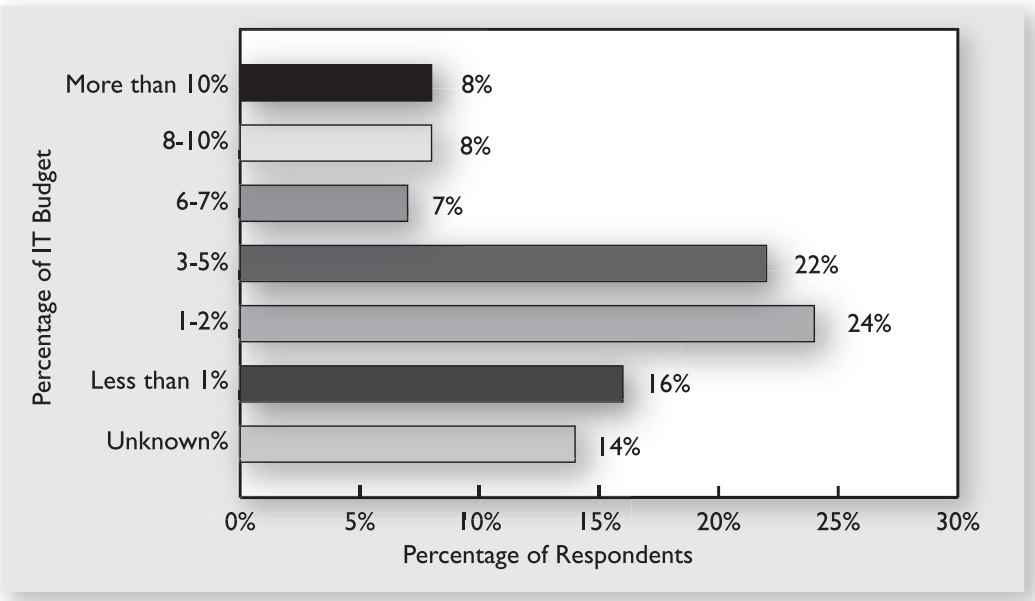


***Figure 5*. Percentage of IT Budget Spent on Security**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

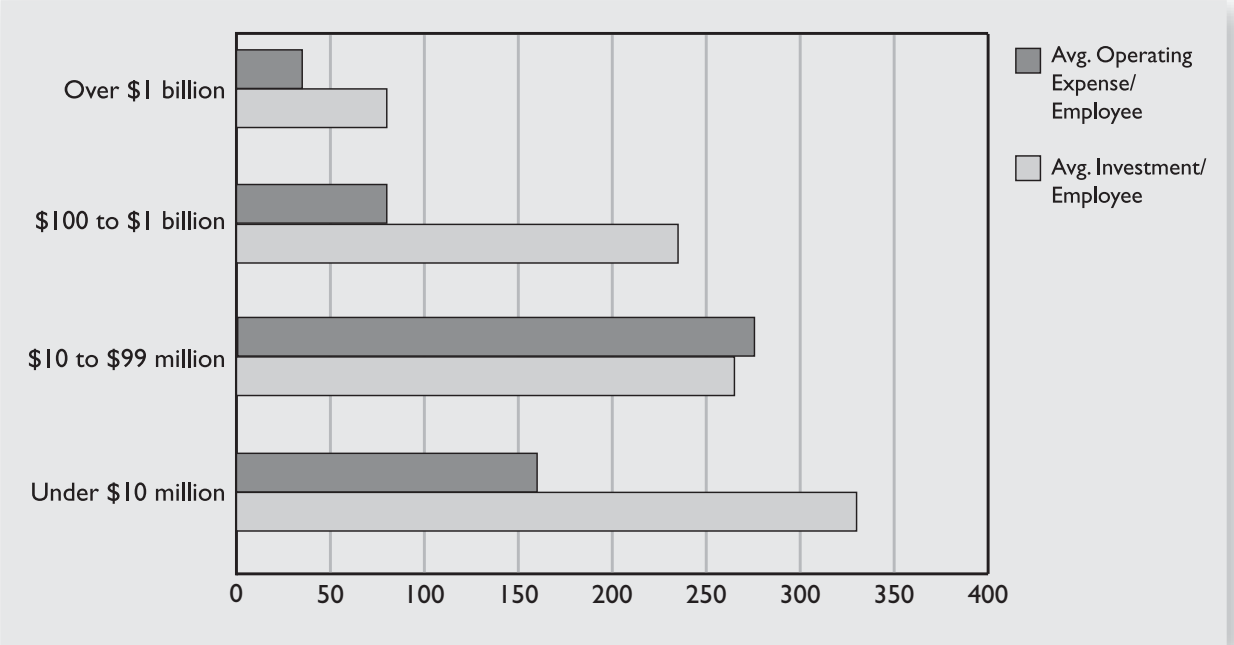
2004: 481 Respondents

the title of system administrator, while 19 percent had various other titles. Given the mission of the Computer Security Institute, it is not surprising that nearly all respondents have crucial information security management responsibilities.

BUDGETING ISSUES

Past CSI/FBI surveys contained a number of questions related to financial aspects of information security, particularly to the costs associated with information security breaches. Over the years, secu-

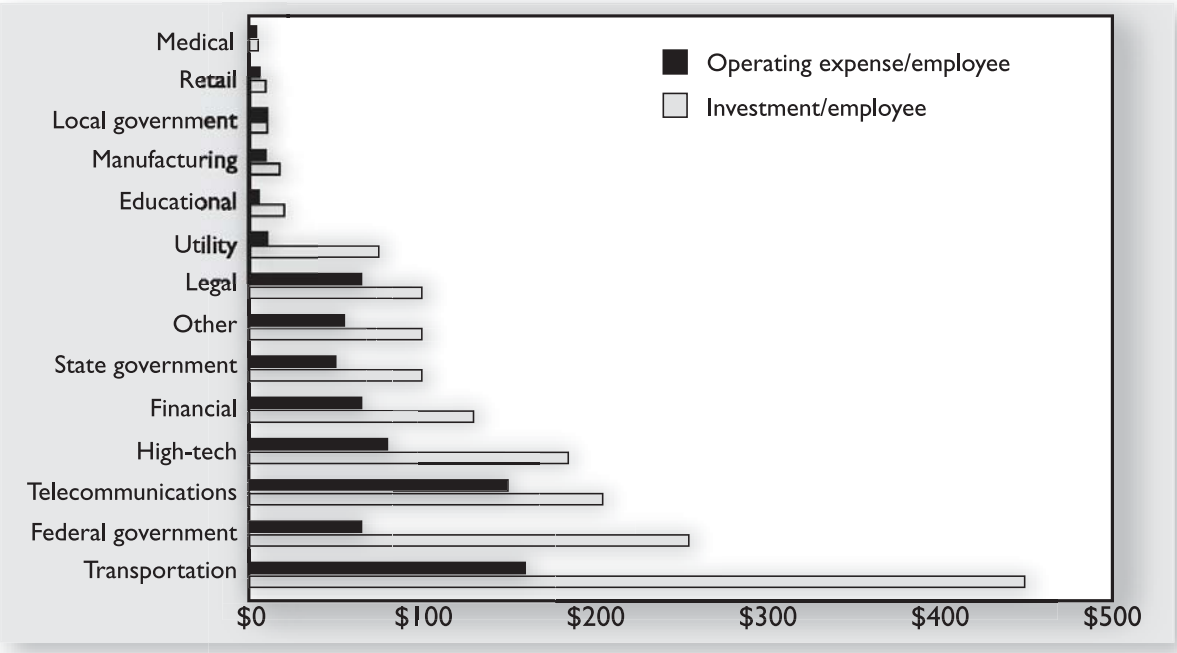
***Figure 6*. Average Reported Computer Security Expenditure per Employee**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: Respondents — Operating Expenditure 302
— Capital Investment 267

Figure 7. **Average Reported Computer Security Expenditure/Investment per Employee**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: Respondents — Operataing Expenditures 302
— Capital Investment 267

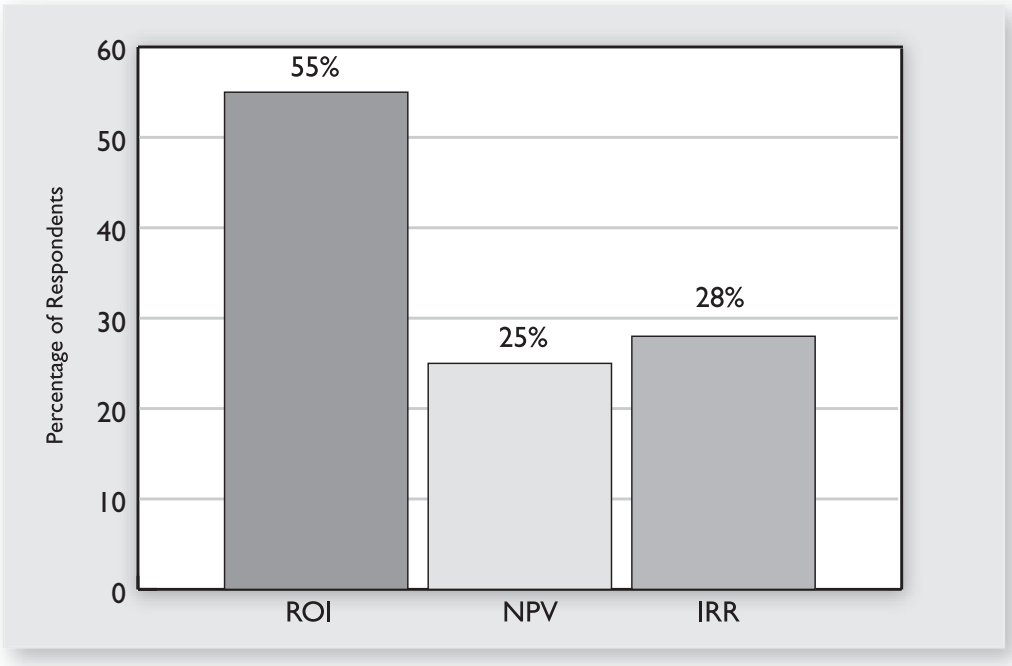
rity managers have become increasingly aware that the financial aspects of information security management demand an increasing portion of their time and effort. Consequently, the 2004 survey was designed to further explore a number of issues related to budgeting and financial management of information security risk.

One new question was aimed at determining the typical size of an organization's information security budget relative to the organization's overall IT budget. As seen in figure 5, 46 percent of respondents indicated that their organization allocated between 1 percent and 5 percent of the total IT budget to security. Only 16 percent of respondents indicated that security received less than 1 percent of the IT budget, 23 percent of respondents indicated that security received more that 5 percent of the budget, while 14 percent of the respondents indicated that the portion was unknown to them.

Additional new survey questions examined the reported average computer security operating expense and investment per employee. One would expect that as a firm's revenue grows, the number of employees would also grow, as would the firm's computer hardware and software needs. Figure 6 is consistent with the notion that as a firm grows, computer security operating and capital expenditures grow less rapidly; i.e., there are economies of scale when it comes to information security. In particular, firm's with annual sales under $10M spent an average of approximately $500 per employee ($334 in operating expense and $163 in capital expenditures) on computer security, while the largest firm's (those with annual sale over $1B), spent an average of about $110 per employee ($82 in operating expense and $30 in capital expenditures).

Spending per employee on computer security is shown in figure 7, broken down by sector for both private and public sector organizations. The highest average computer security spending per employee ($608) was reported by organizations in the transportation sector ($449 of operating expenditures per employee and $159 of capital expenditures per employee). In terms of the operating expenditures on computer security per employee, the next-highest sectors in descending order were the federal government ($261), telecommunications ($209) and high-tech ($183). In terms of the capital expenditures on computer security per employee, the next-highest sectors in descending order were

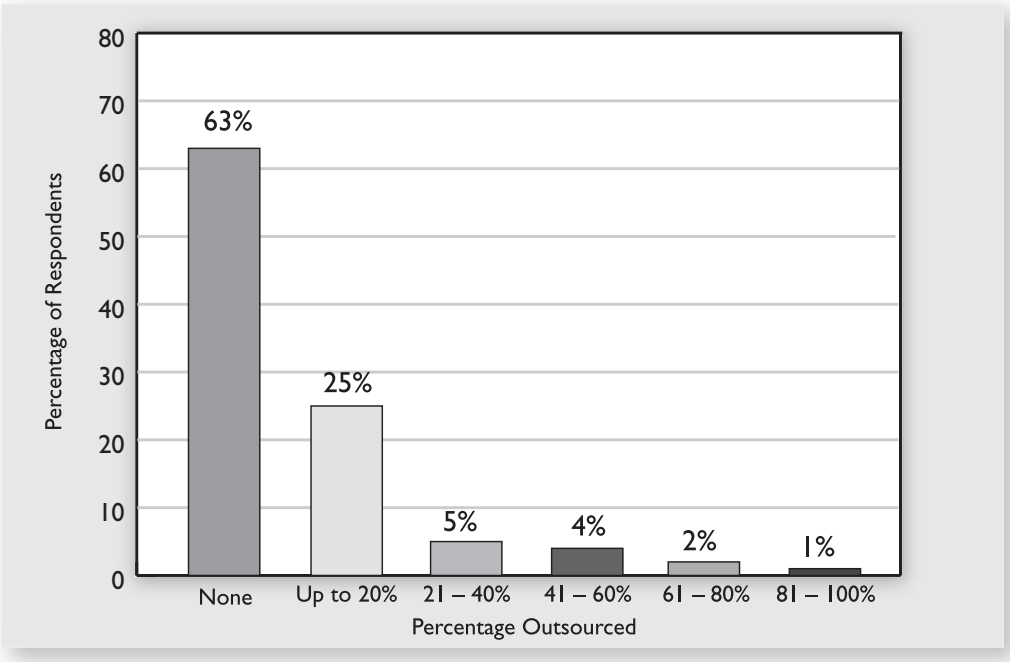
Figure 8. **Percentage of Organizations Using ROI, NPV and IRR Metrics**



2004 CSI/FBI Computer Crime and Security Survey — 2004: 320 Respondents
Source: Computer Security Institute

telecommunications ($150), high-tech ($83), followed by the federal government ($61). It is interesting to note that while the federal government reports among the highest computer security spending per employee, local government reports among the least ($17 per employee for each of operating and capital expenditures), and state governments are somewhere in the middle

Figure 9. **Percentage of Security Function Outsourced**



2004 CSI/FBI Computer Crime and Security Survey — 2004: 478 Respondents
Source: Computer Security Institute

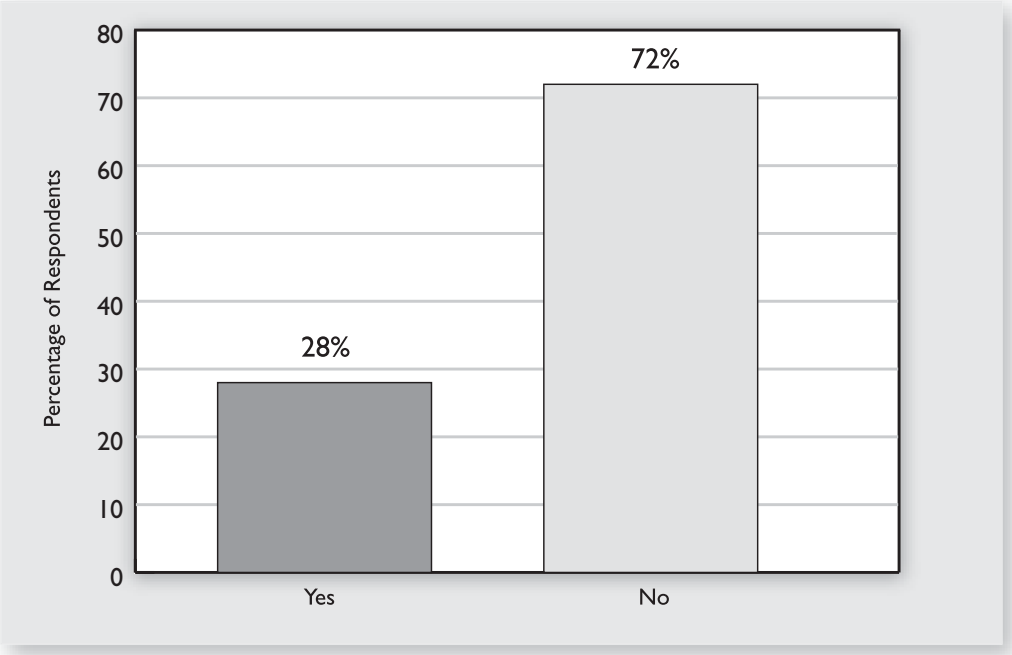
(a total of about $154 combined operating and capital expenditures per employee).

Managers responsible for computer security are increasingly required to justify their budget requests in purely economic terms. There has been considerable discussion of financial metrics used to justify and evaluate investments in computer security at trade and academic meetings, as well as in the computer security journals. Therefore, the 2004 CSI/FBI Survey initiated a new question to determine the popularity of Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as financial metrics for quantifying the cost and benefits of computer security expenditures. In particular, survey participants were asked to indicate on a seven-point scale whether they agree or disagree that their organization uses ROI (NPV, IRR) to quantify the cost/benefit aspects of computer security expenditures. A response of 1, 2 or 3 was interpreted as disagreeing with the statement; a response of 4 was interpreted as neither agreeing nor disagreeing; and a response of 5, 6 or 7 was interrupted as agreeing with the statement. Figure 8 illustrates that 55 percent of respondents indicate their organizations use ROI as a metric, 28 percent use IRR and 25 percent use NPV. Although ROI has a number of limitations when compared with NPV and IRR, ROI is by far the most popular metric used.[2] The significant use of NPV and/or IRR may strike some as surprising, given the oft-heard claim that traditional economic analysis is not applicable to computer security area investments.

Two other new areas of inquiry in this year's CSI/FBI Survey deal with outsourcing cybersecurity and insurance as tool for managing cybersecurity risks. Outsourcing computer security work is not as common as one might suppose. Only 7 percent of respondents indicated that their organizations outsource more than 20 percent of the security function (see figure 9). In contrast, 63 percent of respondents indicated that their organizations do no outsourcing of the security function. It will be interesting to track the outsourcing percentage in future surveys.

Looking at external insurance to manage cybersecurity risks, we found confirmation that it's still early days (figure 10). Technical computer security measures such as the use of passwords, biometrics, antivirus software and intrusion detection systems cannot totally reduce an organization's risk to computer security breaches with their associated

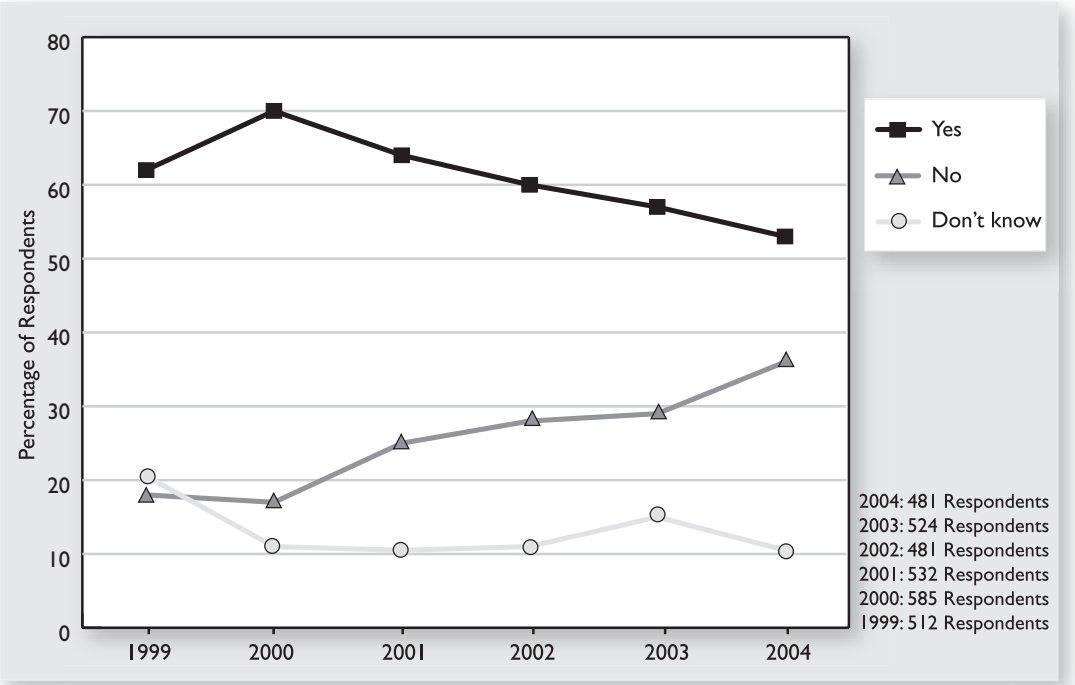
Figure 10. **Does your organization have any external insurance policies to help manage cybersecurity risks?**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 320 Respondents

Figure 11. **Unauthorized Use of Computer Systems within the Last 12 Months**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

Figure 12. **How Many Incidents? From Outside? From Inside?**

How Many Incidents? by percentage	1 – 5	6 – 10	>10	Don't Know
2004	47%	20%	12%	22%
2003	38%	20%	16%	26%
2002	42%	20%	15%	23%
2001	33%	24%	11%	31%
2000	33%	23%	13%	31%
1999	34%	22%	14%	29%
How Many Incidents From the Outside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	9%	9%	30%
2003	46%	10%	13%	31%
2002	49%	14%	9%	27%
2001	41%	14%	7%	39%
2000	39%	11%	8%	42%
1999	43%	8%	9%	39%
How Many Incidents From the Inside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 280 Respondents

financial losses. Hence, it's natural that organizations would turn to insurance to deal with the risk of substantial financial losses that remain after technical security measures have been instituted. Although insurance companies do not currently have good actuarial data on which to base cybersecurity insurance rates, a number of companies do offer such polices.[3] The survey shows, as noted in figure 10, that less than 30 percent of respondents indicated that their organizations use external insurance to help manage cybersecurity risks. As with the question on outsourcing, the response to this new question will provide a baseline reference to judge future trends in an area of receiv-

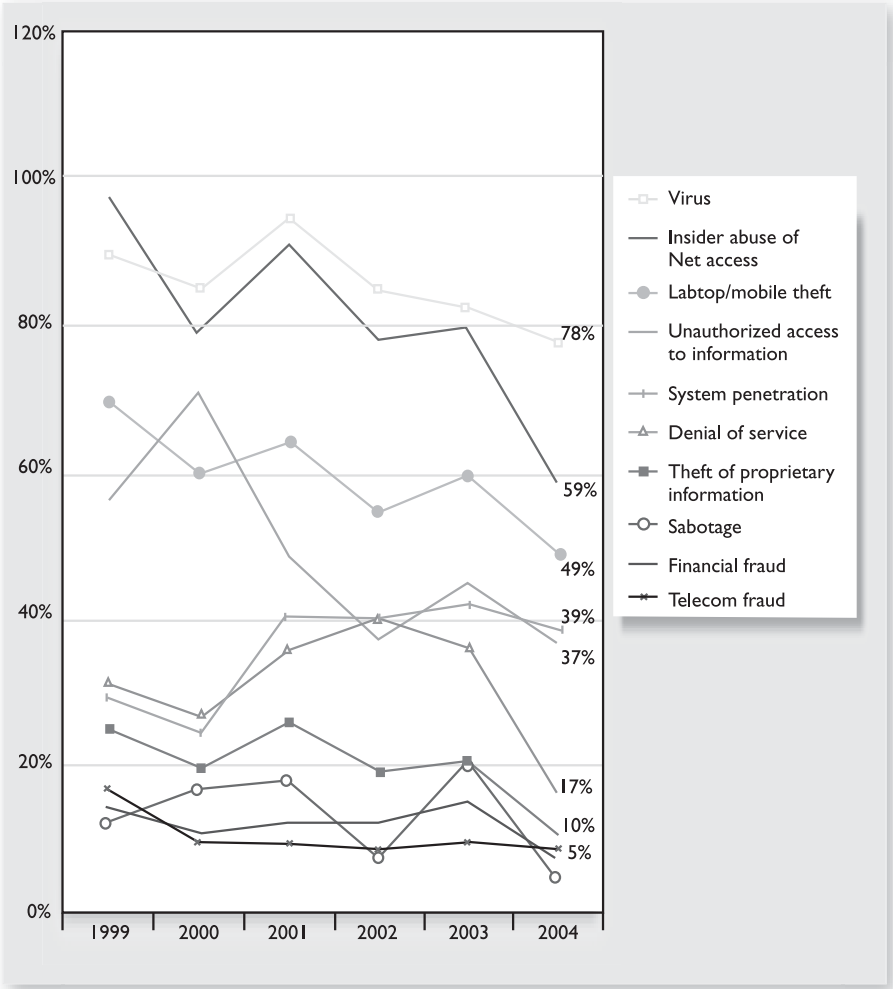
ing considerable interest and discussion in the computer security field.

FREQUENCY, NATURE AND COST OF CYBERSECURITY BREACHES

Turning to figure 11, we can see that the overall frequency of (successful) attacks on computer systems declined this year, a continuing a trend that began in 2001. This year the percentage of respondents answering that their organization experienced unauthorized use of computer systems in the last 12 months declined to 53 percent, the smallest percentage since this question first appeared in the survey in 1999. Moreover, the percentage of respondents answering that there was no unauthorized use of their organization's computer systems increased to 35 percent, as the respondents not knowing if such unauthorized use occurred dropped to a low of 11 percent.

Figure 12 also demonstrates that cybersecurity breaches are declining, and the source of the breaches appears fairly evenly split between those originating on the outside and those originating within the organization. Over the years, the first panel of figure 12 shows that the percentage of respondents estimating that their firm experienced between six and ten computer security incidents within the previous year appears to have leveled off at 20 percent, while the percentage of respondents estimating that their firm experienced between one and five computer security incidents increased to 47 percent. This year showed the lowest percentage (12 percent) of respondents estimating that organization experienced more than ten computer security incidents during the past year.

***Figure 13*. Types of Attacks or Misuse Detected in the Last 12 Months (by percent)**



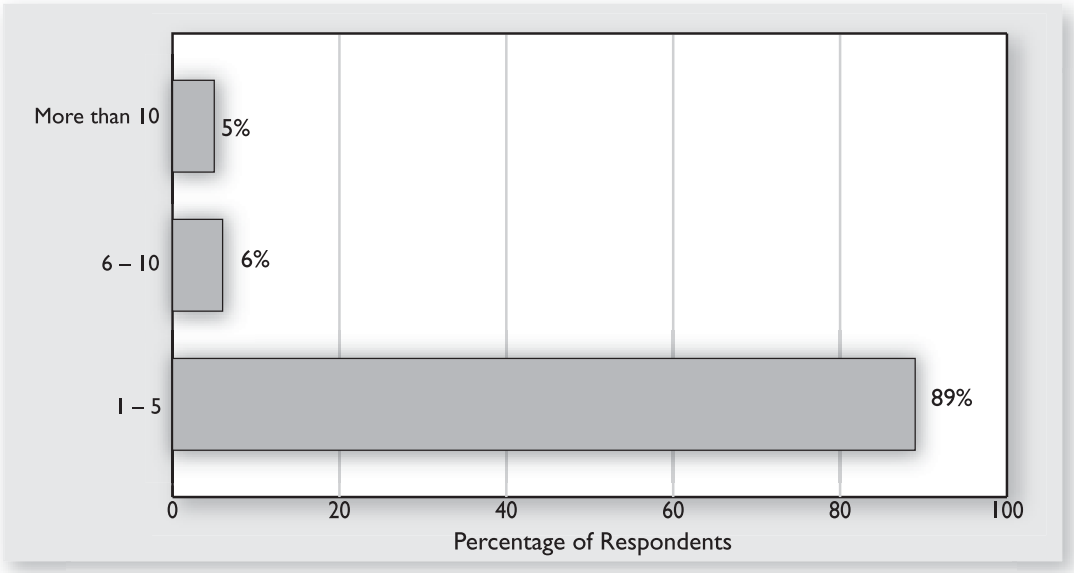
2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 481 Respondents

Figure 13 provides a visual demonstration that attacks of computer systems or (detected) misuse of these systems has been slowly, but fairly steadily decreasing over many years in nearly all categories. As seen in the figure, there has been a dramatic drop in reports of system penetrations, insider abuse, and theft of proprietary information. Three new categories were added to this year's survey, and obviously trend data is not available. However, for this year's survey, 15 percent of the respondents reported abuse of wireless networks, 7 percent reported Web site defacement, and 10 percent reported misuse of public Web applications.

All the organizations covered by this year's survey experienced some

Figure 14. **Percentage Experiencing Web Site Incidents**



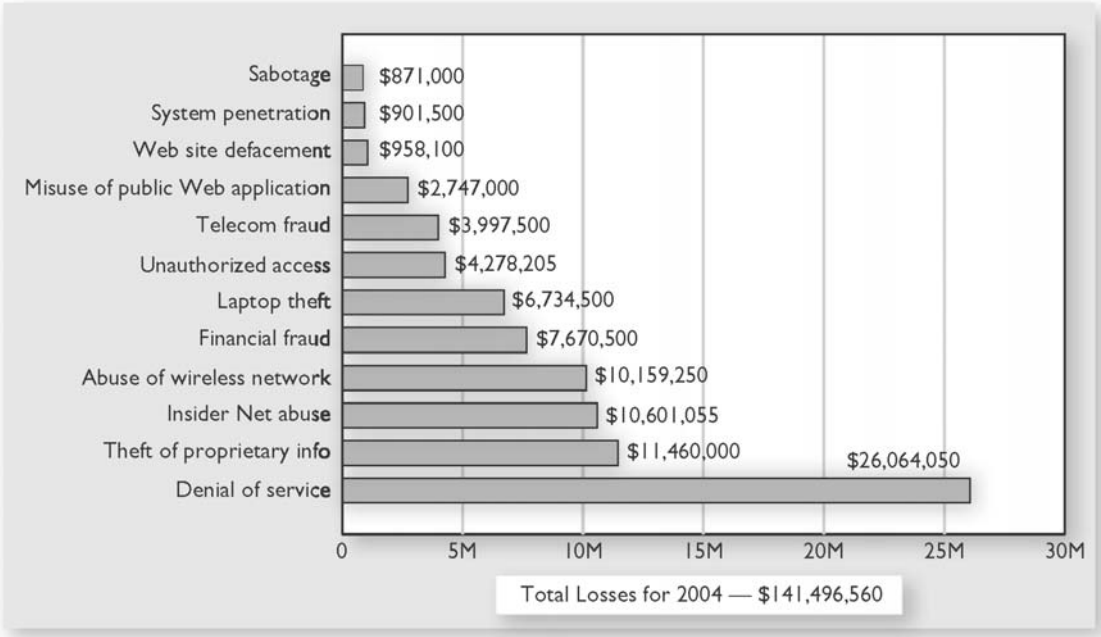
2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 132 Respondents

Web site incidents. This is seen in figure 14, which also shows that only 5 percent of respondents reported that their organizations experienced more than ten Web site incidents. The vast majority (89 percent) of respondents indicated that their organizations experienced between one and five Web site incidents in the previous twelve months.

Respondents' estimates of the losses caused by type of computer security incident are shown in figure 15. A number of important points are related to figure 15, some of which are not readily accessible from inspection of the figure. First, the real story of losses is that the total losses reported (on a per respondent basis) declined. Although the dollar amounts/employee were not available from previous surveys, total losses for 2004 were $141,496,560, down from $201,797,340 in 2003. Second, as in the past, respondents are generally ei-

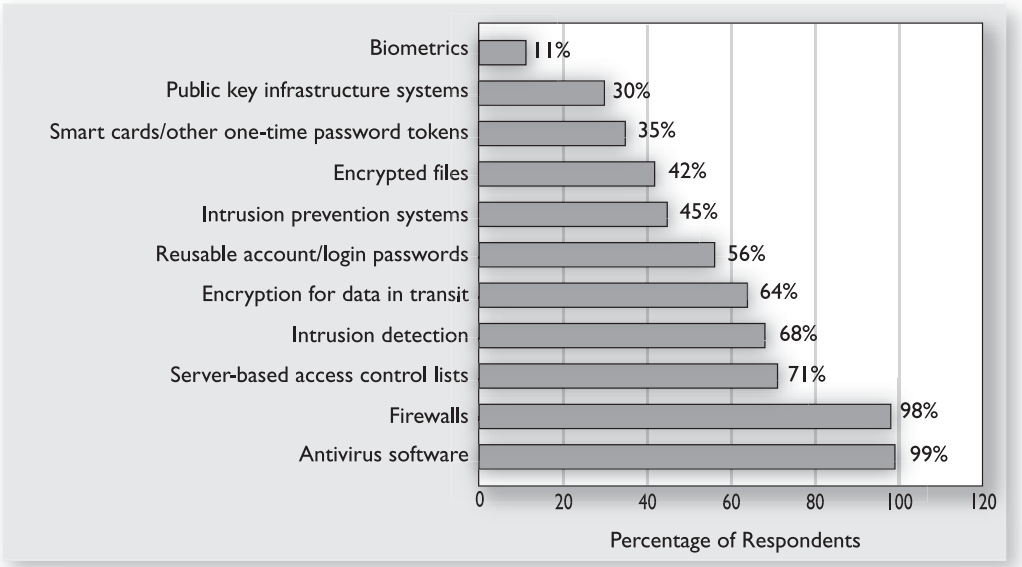
Figure 15. **Dollar Amount of Losses by Type**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Figure 16. **Security Technologies Used**



ther unable or unwilling to estimate the dollar losses. In this year's survey, 269 respondents out of a total of 494 provided dollar loss estimates. Third, the denial of service category emerged for the first time as the incident type generating the largest total losses (replacing theft of proprietary information, which had been the most expensive category of loss for five consecutive years). To the extent that this result can be generalized to the whole population, it may be due to last year's rise in the degree to which virus threats were entwined with denial of service attacks (witness the numerous variants of the MyDoom worm, which carried as its payload a time-triggered denial of service attack program).

SECURITY TECHNOLOGIES USED

As in previous years, survey takers were asked to identify the types of security technology used by their organizations. This year's survey, however, updated the categories, clarifying and adding some, and eliminating others (see figure 16).

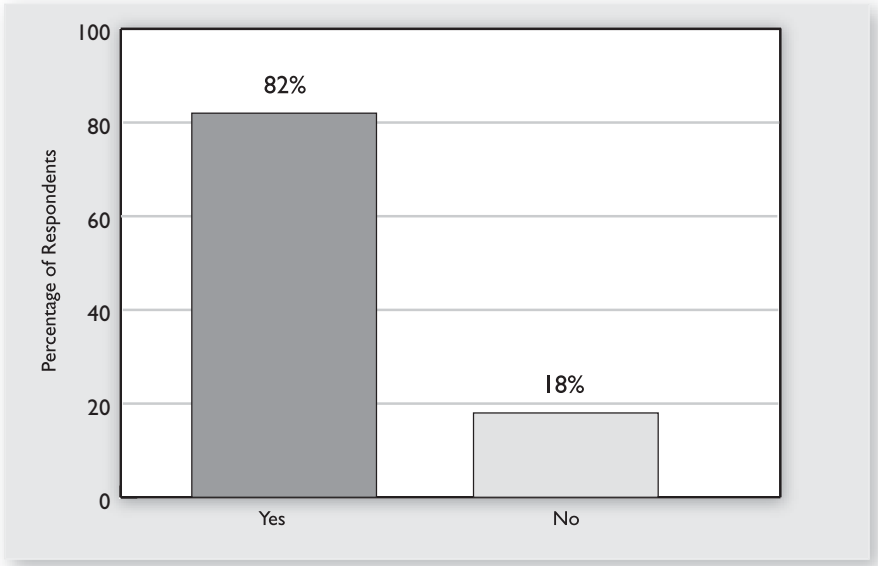
Several categories addressed systems defending against network attack. As in previous years, antivirus software was reported as being used by 99 percent of the organizations. Nearly all organizations, 98 percent, also reported using firewalls. Intrusion detection systems were being used by 68 percent of the organizations (a 5-percent drop from last year), while 45 percent of the respondents' organizations jumped on the intrusion prevention system bandwagon. Intrusion prevention systems attempt to identify and block malicious network activity in real time. Although these systems look like firewalls they work differently—firewalls block all traffic except that which they have a reason to pass, while intrusion prevention systems pass all traffic unless they have a reason to block it.

Several categories shown in figure 16 deal with access control. Server-based access control lists were reported to be used by 71 percent of the respondents. Reusable account/login passwords was reported to be used by 56 percent, the use of smart cards and other one-time password tokens used was claimed by 35 percent, and biometrics remained flat at 11 percent. Measures to protect information while in transit included encryption of data in transit, reported to be used by 64 percent of respondents, use of encrypted files at 42 percent, and use of public key infrastructure system at 30 percent.

SECURITY AUDITS AND SECURITY AWARENESS TRAINING

Several new questions in this year's survey dealt with various aspects of improving computer security (beyond the use of technologies discussed above). Although the industry literature long has suggested using an audit as the first step toward a meaningful information security program, no data had been collected concerning the use of security audits prior to this year's survey. Make no mistake: audits are widely used, just as the textbooks prescribe. Figure

Figure 17. **Does your organization conduct security audits?**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute
2004: 470 Respondents

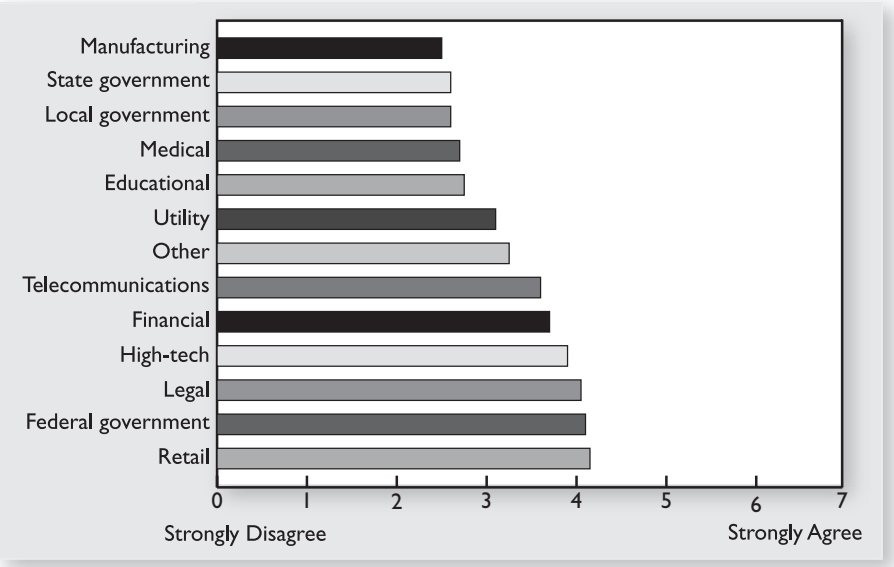
17 shows that 82 percent of respondents indicated that their organizations conduct security audits.

There's a noticeable flip side to this statistic, however. While the vast majority of organizations surveyed do use computer security audits, it is a bit surprising that use of security audits is far from universal. Future surveys will help determine if there is a trend in security audit use.

In addition to proposing the use of security audits, the computer security literature makes it clear that organizations should supplement technological security measures with investments in security training. Two new questions in this year's survey address the extent and importance of security awareness training. First, respondents were asked to rate the degree to which they agreed with the statement, "My organization invests the appropriate amount on security awareness." Figure 18 illustrates that, on average, respondents from all sectors do not believe that their organization invests enough in security awareness.

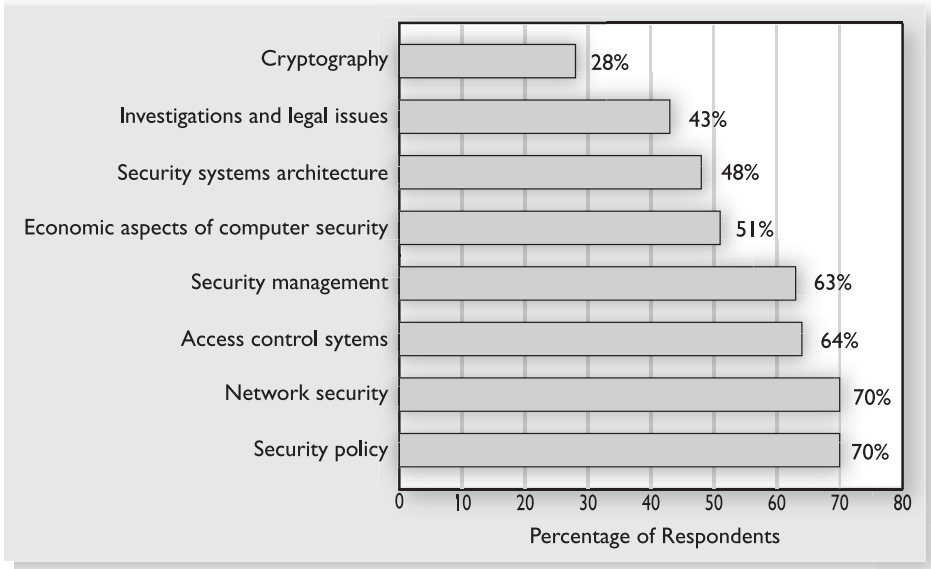
Survey participants were also asked to rate the importance of security awareness training to their organizations in each of several areas. Figure 19 shows the percentages of respondents indicating that security awareness was very important (as measured by importance ratings of five or above on seven-point scale) in the various areas of security. For five of the eight security areas listed, the average rating indicated that training for that area was very important. Security awareness training was perceived most valuable in the areas of security policy (70 percent) and network security (70 percent), followed by access control systems (63 percent), security management (62 percent), and economic aspects of computer security (51 percent). The three areas in which security awareness was perceived to be the least valuable were security systems architecture (47 percent), investigations and legal issues (43 percent) and cryptography (28 percent).

Figure 18. **Organization Invests an Appropriate Amount on Security Training: Mean Values Reported on a Seven-Point Scale**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute
2004: 488 Respondents

Figure 19. **Importance of Security Awareness Training: Percentage of Respondents Identifying as Important**



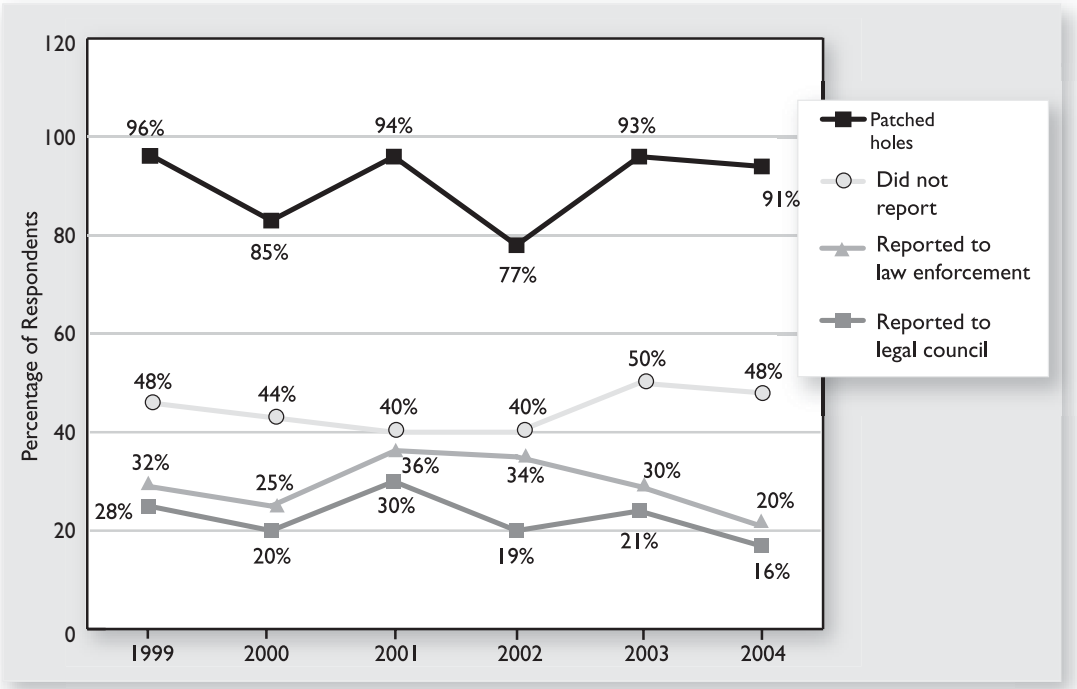
2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 480 Respondents

INFORMATION SHARING

Although information sharing has recently been promoted by the Department of Homeland Security and various leaders in the computer security community, this year's CSI/FBI Computer Crime and Security Survey detected no increase in the disposition to share information about security intrusions. Figure 20 shows how the organizations surveyed responded to computer intrusions in each year of the survey beginning with 1999. The top line shows that more than 90 percent of respondents indicated that their organization responds by patching security holes. The high percentage of organizations that react by patching holes has remained high through the years, and only once dipped below 80 percent. The next line down in the figure shows that only half of all respondents indicated that their orga-

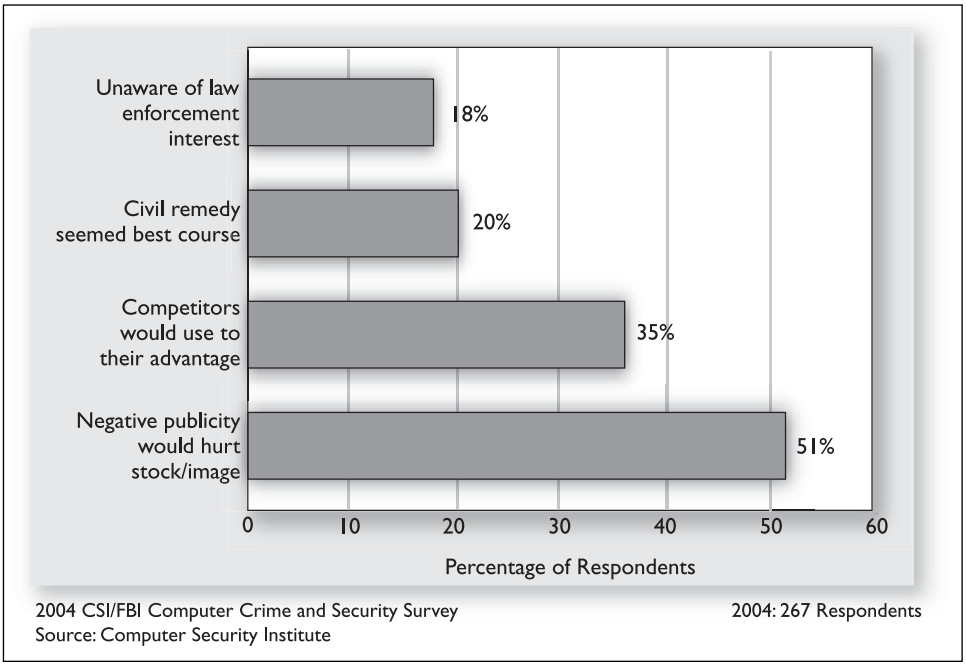
Figure 20. **If your organization has experienced computer intrusion(s) within the last 12 months, which of the following actions did you take?**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 320 Respondents

Figure 21. **Reason organization did not report intrusion to law enforcement: Percentage of respondents identifying as important**

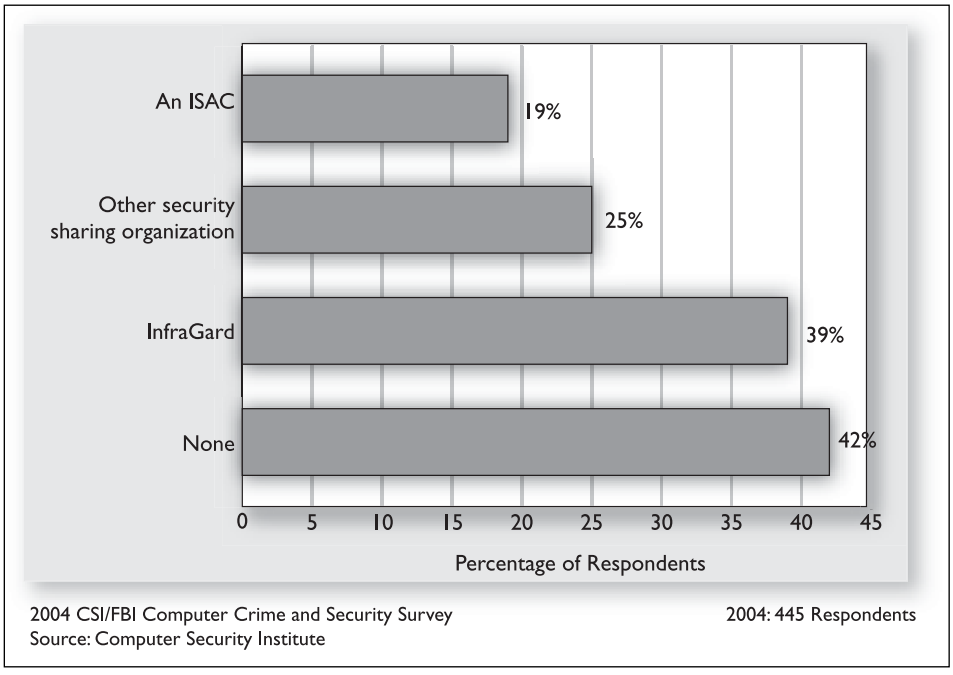


nization shares information about a security breach. The percentage sharing did not increase in the past year, and remains at virtually the same level as in the 1999 survey. Surprisingly, as shown by the third line down in figure 20, the latest year shows a noticeable downturn in the percentage of organizations that reported computer intrusions to law enforcement.

Figure 21 summarizes the reasons why organizations did not report intrusions to law enforcement. This figure shows the percentages of respondents identifying each stated reason as being very important (as measured by an importance rating of five or above on a seven-point scale) in the decision not to report the computer intrusion. Over 50 percent of respondents (of those indicating that their organizations would not report an intrusion to law enforcement) cited as very important the perception that the negative publicity would hurt their organization's stock and/or image.[4] Nearly 35 percent of respondents cited the advantage competitors could use as very important. Only 20 percent of respondents thought that using a civil remedy was a very important reason for not reporting the intrusion. Less than one of five respondents claimed that being unaware of law enforcement's interest in the breach was a very important reason for failure to report the intrusion. In other words, organizations are aware, by and large, of law enforcement's role in combating computer security crime, but choose nonetheless not to report most computer crimes.

To add depth to our understanding of information sharing among respondents, the survey this year also asked if organizations belong to an information sharing organization. Although some organizations belong to multiple sharing groups, you can see from

Figure 22. **Percentage of organizations that belong to an information sharing organization**



the bottom bar in figure 22 that about 57 percent of the respondents indicated that their organizations do not belong to any information sharing organization. About 38 percent of organizations in the survey belong to InfraGard, 18 percent belong to an ISAC, and 26 percent to some other security sharing organization. Overall, the survey results concerning the willingness of organizations to participate fully in information sharing of security breaches is consistent with recent theoretical work by academicians.[5]

EFFECT OF SARBANES-OXLEY ACT

Finally, this year's survey introduced a new question to determine the effect, if any, of the Sarbanes-Oxley Act on the information security activities. As shown in figure 23, the respondents in the financial, utility and telecommunications sectors believe the Sarbanes-Oxley Act is having an impact on their organizations' information security. In contrast, however, most of the respondents in the other sectors did not agree that the Sarbanes-Oxley Act either raised the level of interest in information security in their organizations or shifted the focus in their organizations from technology to corporate governance. Of course, due to the phasing-in nature of the Act, we will have to wait for next year's survey results to assess the full impact of the Sarbanes-Oxley Act on information security.

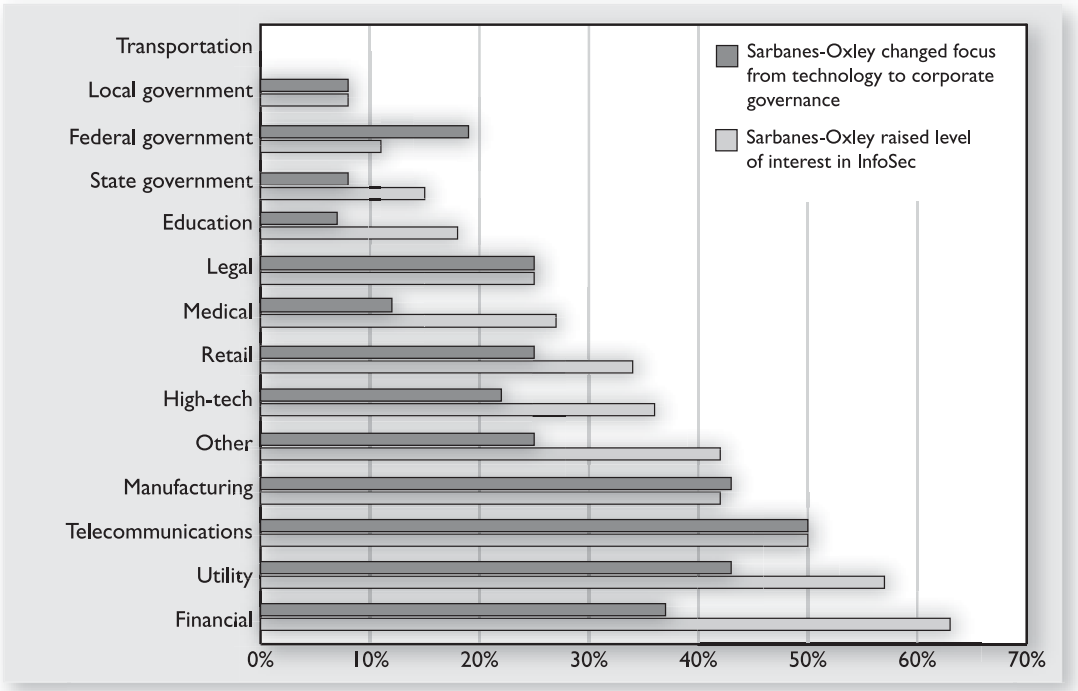
CONCLUDING COMMENTS

Computer-based information systems have been of critical importance to most major organizations for several decades. Since the mid-1990s, the Internet has solidified the central role of computers in the functioning of modern organizations. Concern with computer security has also moved to center stage since the emergence of the Internet.

Computer security has focused on several issues over the years. In the initial stages, computer security focused largely on technical issues like encryption, access controls and intrusion detection systems. More recently, as highlighted by the results of this year's CSI/FBI Computer Crime and Security Survey, economic, financial and risk management aspects of computer security have also become important concerns to today's organizations. These latter concerns are complements to, rather than substitutes for, the technical aspects of computer security.

The more knowledge we have about the causes and consequences of computer security breaches, as well as the way organizations address computer security issues, the more likely it is that computer security will improve. The survey results presented in this report represent what we hope to be valuable additions to this required knowledge base. As with earlier CSI/FBI Computer Crime and Security Surveys, the

***Figure 23*. Sarbanes-Oxley Act impact on information security: Percentage of respondents that agree**



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 464 Respondents

overall objectives underlying this year's survey are to assess the key trends surrounding computer security and to identify important changes emerging on the computer security landscape. Future CSI/FBI surveys will continue to focus on these twin objectives.

A NOTE FROM ROBERT RICHARDSON, CSI'S EDITORIAL DIRECTOR

CSI offers the survey results as a public service. The report is free at the CSI Web site (GoCSI.com).

The participation of the FBI's San Francisco Computer Crime Squad office has been invaluable. Over the years, the squad has provided input into the development of the survey and acted as our partners in the effort to encourage response. This year, Special Agent Shelagh Sayers was instrumental in providing insight for the newly developed survey questions. We should note, however, that CSI has no contractual or financial relationship with the FBI. The survey is simply an outreach and education effort on the part of both organizations. CSI funds the project and is solely responsible for the results.

New to the undertaking this year, as readers will certainly already have noticed, is the involvement of three academicians (their biographies are below) who specialize in the economics of information security. These three have graciously joined me in coauthoring this report. Both I and the entire CSI team thank the academic team of Gordon, Loeb and Lucyshyn and look forward to future collaborations.

Opinions offered in the this report are those of the authors and not necessarily those of the Federal Bureau of Investigation, Computer Security Institute, or any other organization.

About the Authors: Lawrence A. Gordon is the Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance in the Robert H. Smith School of Business at the University of Maryland (lgordon@rhsmith.umd.edu). Martin P. Loeb is Professor of Accounting and Information Assurance and Deloitte & Touche Faculty Fellow in the Robert H. Smith School of Business at the University of Maryland (mloeb@rhsmith.umd.edu). William Lucyshyn is Visiting Senior Research Scholar in the School of Public Affairs at the University of Maryland (Lucyshyn@umd.edu). Robert Richardson is Editorial Director at the Computer Security Institute (rrichardson@cmp.com).

NOTES

[1] For an overview of the impact of economics on information security, see Lawrence A. Gordon and Robert Richardson, "The New Economics of Information Security," *InformationWeek*, March 29, 2004, pp. 53-56.

[2] For a discussion of the limitations of ROI, see Lawrence A. Gordon and Martin P. Loeb, "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance*, November 2002, pp. 26-31.

[3] For examples of such insurance firms and further analysis of cybersecurity insurance, see Lawrence A. Gordon, Martin P. Loeb Gordon, and Tashfeen Sohail, "A Framework for Using Insurance for Cyber Risk Management," *Communications of the ACM*, March 2003, pp. 81-85.

[4] This is consistent with recent research by Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou ("The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, Vol. 11, No. 3, 2003, pp. 431-448) that found reports of security breaches can adversely affect a firm's stock price.

[5] See Lawrence A. Gordon, Martin P. Loeb Gordon, and William Lucyshyn, "Sharing Information on Computer Systems: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol. 22, No. 6, 2003, pp. 461-485.

Contact Information

For referrals on specific criminal investigations:
Shelagh Sayers, Special Agent
San Francisco FBI Computer Crime Squad
(415) 553-7400
san.francisco@fbi.gov, subject line: CSI Report
For general information: www.nipc.gov

For information on the CSI/FBI study:
Robert Richardson, Editorial Director
Computer Security Institute
610-604-4604
rrichardson@cmp.com
For general information: GoCSI.com

How CSI Can Help

The results of this survey clearly indicate that the stakes involved in information systems security have risen. Your organization is vulnerable to numerous types of attack from many different sources and the results of an intrusion can be devastating in terms of lost assets and good will. There are steps you can take to minimize the risks to your information security and Computer Security Institute can help.

Computer Security Institute (CSI) is the world's premier membership association and education provider serving the information security community, dedicated to advancing the view that information is a critical asset and must be protected. Through conferences, seminars, publications and membership benefits, CSI has helped thousands of security professionals gain the knowledge and skills necessary for success. For 31 years, CSI conferences and training have won the reputation as being the most well-respected in the industry.

As a member of CSI you are linked to a high-powered information source and an organization dedicated to providing you with unlimited professional development in one package.

Contact CSI
Phone 415-947-6320
Fax 415-947-6023
E-mail csi@cmp.com
GoCSI.com

Conferences:

31st Annual Computer Security Conference & Exhibition
November 8-10, 2004, Washington, D.C.
The world's largest conference devoted to computer and information security

NetSec 2005
June 13-15, 2005, Scottsdale, AZ
A balanced perspective of managerial and technical issues makes this the most popular conference devoted to network security.

32nd Annual Computer Security Conference & Exhibition
November 14-16, 2005, Washington, D.C.

Training on a wide variety of topics including:

- Awareness
- Policies
- Intrusion Prevention
- Risk Analysis
- Social Engineering
- Wireless Security

FrontLine End User Awareness Newsletter

TopLine Executive Newsletter

Working Peer Groups

Membership Benefits:

- Computer Security *Alert*
- Computer Security Journal (quarterly)
- SecurCompass® Automated Standards-based Program Assessment and Design Tool
- Discounts on conferences, training and publications

Not a CSI member? To start receiving the Alert, Computer Security Journal and other Membership benefits, go to GoCSI.com or call 866-271-8529.

CSI
COMPUTER SECURITY INSTITUTE