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.

DETAILED SURVEY RESULTS

NOTE: Dates on the figures refer to the year of the report (i.e., 2006). The supporting data is based on the 2005 calendar year.

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 through 4. To encourage respondents to share information about occasions when their defenses were overrun and, in particular, to provide data regarding financial damages, the survey is conducted anonymously. A necessary result of this is that direct longitudinal analyses are not possible. Generally speaking, however, the demographics of survey respondents have remained consistent over the past several years, making it reasonable to draw some conclusions regarding trends in the year-over-year data.

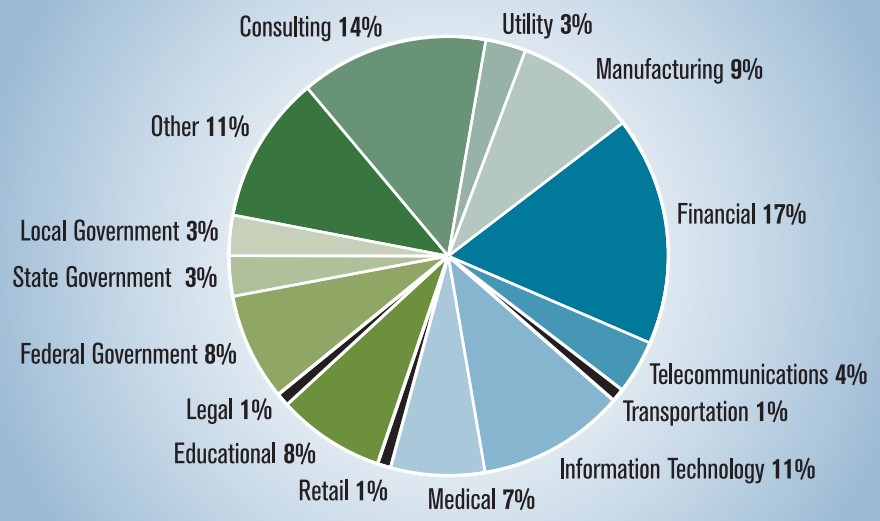
Respondents are drawn from a pool of U.S.-based members of the Computer Security Institute (CSI), a 33-year-old professional organization for information security professionals. Details on survey methodology can be found on page 26.

As **figure 1** shows, organizations covered by the survey include many areas from both the private and public sectors. The sectors with the largest number of responses came from finance (17 percent), followed by consulting (14 percent), information technology (11 percent) and manufacturing (9 percent). The portion coming from government agencies (combining federal, state and local levels) was 14 percent, and educational institutions accounted for 8 percent of the responses. The diversity of organizations responding was also reflected in the 11 percent designated as "other." The proportion of respondents coming from the various sectors remains roughly the same as in previous years.

Figure 2 (page 4) shows that the survey pool leans toward respondents from large enterprises. Organizations with 1,500 or more employees accounted for a little 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

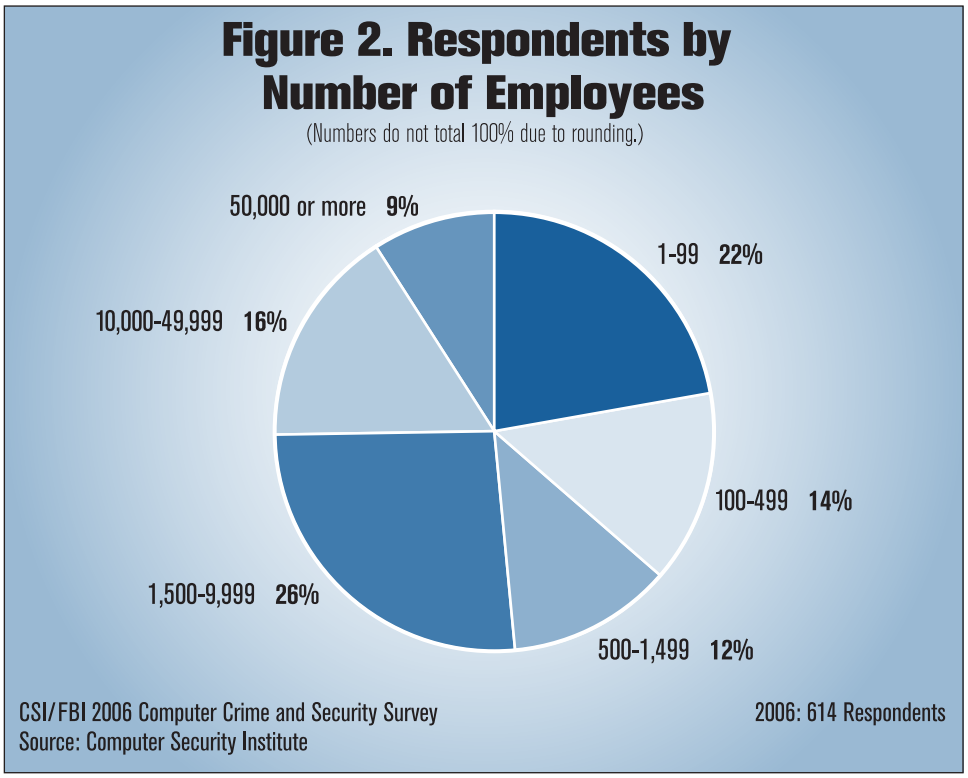
Figure 1. Respondents by Industry Sector

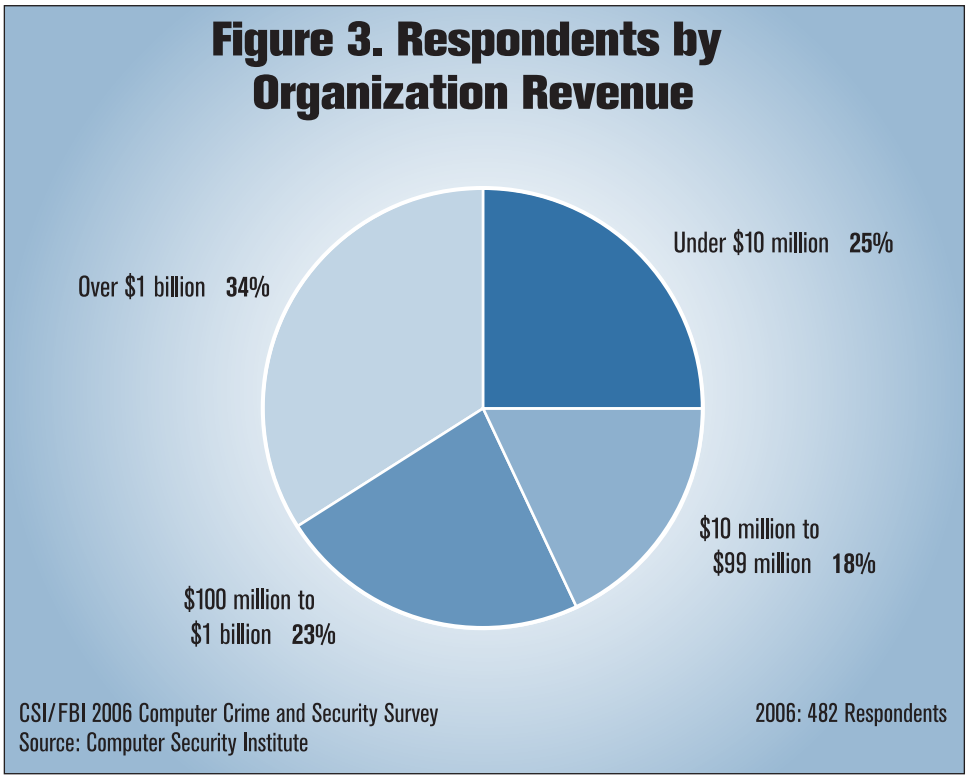
(Numbers do not total 100% due to rounding.)



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 615 Respondents





accounted for 26 percent of all responses. The category covering the largest organizations, those with 50,000 or more employees, made up 9 percent of all responses. As in the past, a substantial minority of responses (22 percent this year, compared to 20 percent last year) came from firms having fewer than 100 employees—the "small business" point of view is covered here, though not proportionally to the overall number of small organizations in the United States.

Figure 3 shows the composition of the responding commercial enterprises by the annual revenue they generated. The largest firms in America are well-represented in our survey findings, since 57 percent of the firms responding generated annual revenues in excess of $100 million, including 34 percent generating annual revenues in excess of $1 billion. Nevertheless, 25 percent of the responding firms generated annual revenues under $10 million. Comparing these numbers with our earlier surveys, one sees that roughly the same size firms responded over

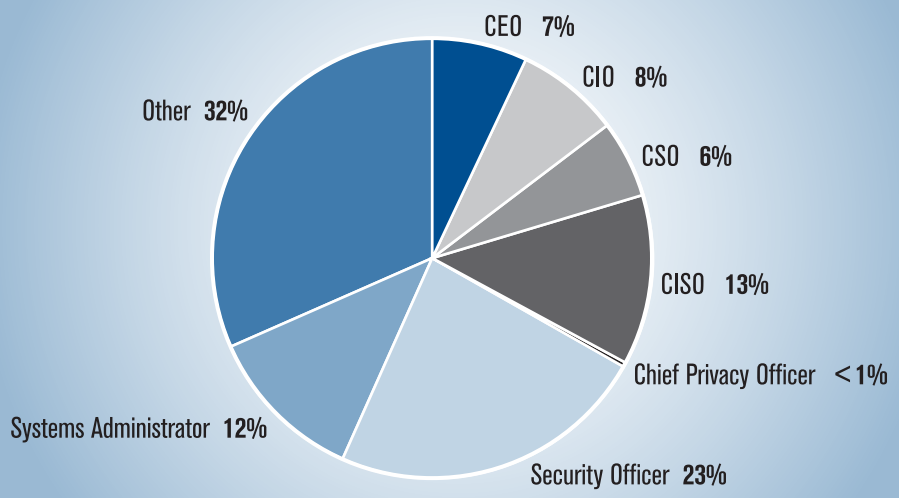
time—again allowing us to make some meaningful trend analyses.

For the third consecutive year, the survey categorized respondents by job title. **Figure** 4 illustrates that 34 percent of the respondents were senior executives with the titles of chief executive officer (CEO) (7 percent), chief information officer (CIO) (8 percent), chief security officer (CSO) (6 percent) or chief information security officer (CISO) (13 percent). The single largest category of respondents (23 percent) had the job title of security officer. An additional 12 percent of respondents had the title of system administrator, while 32 percent had various other titles. This year's questionnaire also included a checkbox for chief privacy officer, but clearly the title is not enjoying widespread use, as only two respondents indicated having this title. The large "Other" category (32 percent this years versus 35 percent last year) reflects the great diversity in titles in the information security arena.

One final point to be made about the survey

Figure 4. Respondents by Job Description

(Numbers do not total 100% due to rounding.)



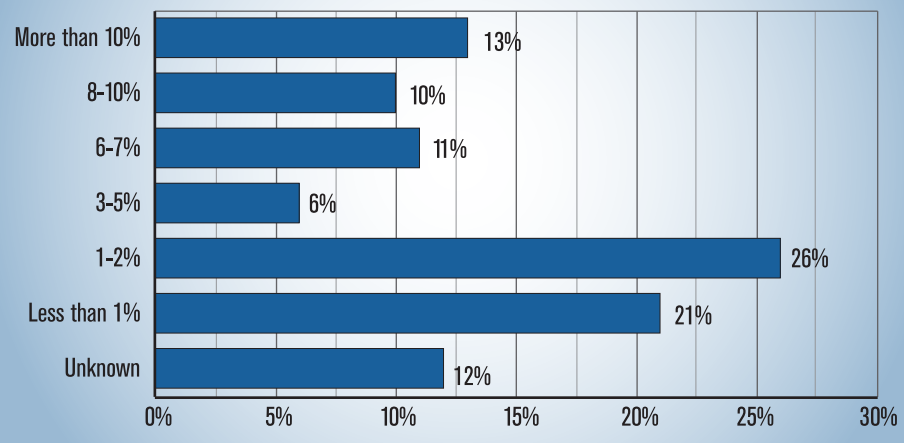
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 614 Respondents

Figure 5. Percentage of IT Budget Spent on Security

By Percent of Respondents

(Numbers do not total 100 % due to rounding.)

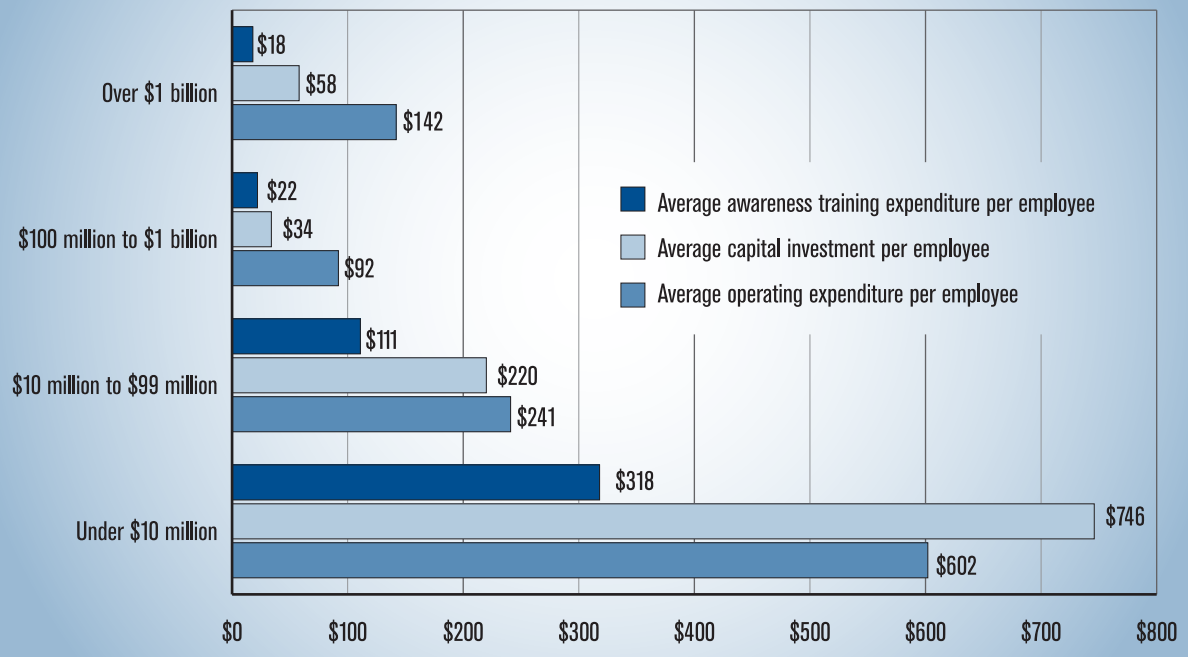


CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 613 Respondents

Figure 6. Average Reported Computer Security Expenditure Per Employee

By Organization Revenue



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 290 Respondents

pool is that it very likely skews toward respondents who have an above-average interest in information security; this because all respondents are either members of the Computer Security Institute or have been paid attendees at CSI conferences and training events. It is reasonable to assume, thus, that they are more "security savvy" than would be a survey pool of randomly selected information technology professionals.

Budgeting Issues

For the third consecutive year, the survey explored a number of issues related to budgeting and financial management of information security risk.[1] First, respondents provided information concerning the relative portion of their organizations' IT budget that is devoted to information security activities. **Figure 5** (page 5) illustrates that 47 percent of respondents indicated that their organization allocated less than 3 percent of the total IT budget to security, which compares to 35 percent in last year's survey. However, 34 percent of respondents indicated that their organization allocated more that 5 percent to security, and this compares to 27 percent in last year's survey. The percentage of respondents indicating that their organizations allocate between 3 and 5 percent of their IT budgets to security

1. Of course, the CSI/FBI surveys have always contained a number of questions related to the costs associated with information security breaches.

activities declined from 24 percent last year to only 6 percent this year, indicating a shift to both higher and lower extremes.

Beginning with the 2004 report, the survey examined the reported average computer security operating expense and investment per employee. The 2006 questionnaire also probed the average awareness training expenditures per employee. As can be seen from **figure 6** (page 6), the average awareness training expenditures per employee decrease with an organization's size. The smallest organizations, those with revenues of less than $10 million, spend $318 per employee and the largest organizations, those with annual revenues of over $1 billion, spend $18 per employee. Thus, there appear to be economies of scale in providing awareness training. The average computer security operating expense and investment per employee—consistent with last year's results—initially displays economies of scale and then, diseconomies of scale. In particular, the average information security expenditure and investment per employee decreases as the organizations get larger, but then increases when moving to the largest organizations (those with over $1 billion in revenue).

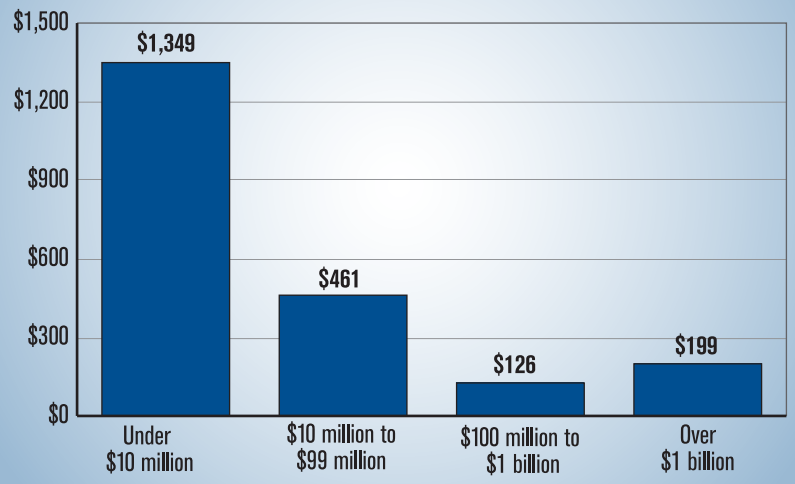
The same behavior can easily be seen (**figure** 7) for total security expenditures and investments per employee (i.e., average operating expense per employee + average investment per employee). In particular, firms with annual sales under $10 million spent an average of approximately $1,349 per employee ($602 in operating expense and $746 in capital expenditures + $1 due to rounding) on computer security—a 210 percent increase over 2005. Firms with annual sales between $10 million and $99 million, spent an average of approximately $461 per employee ($241 in operating expense and $220 in capital) on computer security—a 327 percent increase over 2005. Firms with annual sales between $100 million and $1 billion spent an average of approximately $126 per employee ($92 in operating expense and $34 in capital expenditures) on computer security—a 62 percent reduction over 2005. The largest firm's (those with annual sales over $1 billion), spent an average $199 per employee ($142 in operating expense and $58 in capital expenditures - $1 due to rounding) on computer security, a 19 percent reduction over 2005.

For some time now, it has generally been believed that projects designed to increase an organization's information security will not automatically be approved by senior management (e.g., by the chief financial officer), but instead need to be justified in economic terms. Hence, starting in 2004, a question was added to determine the popularity of Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as

Figure 7. Combined Average Reported Computer Security Expenditure Per Employee

By Organization Revenue

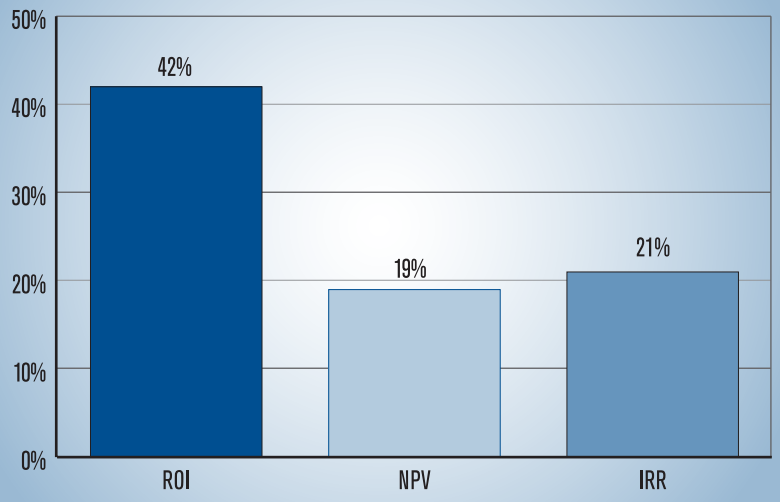
(Does not include awareness training expenditures.)



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 290 Respondents

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

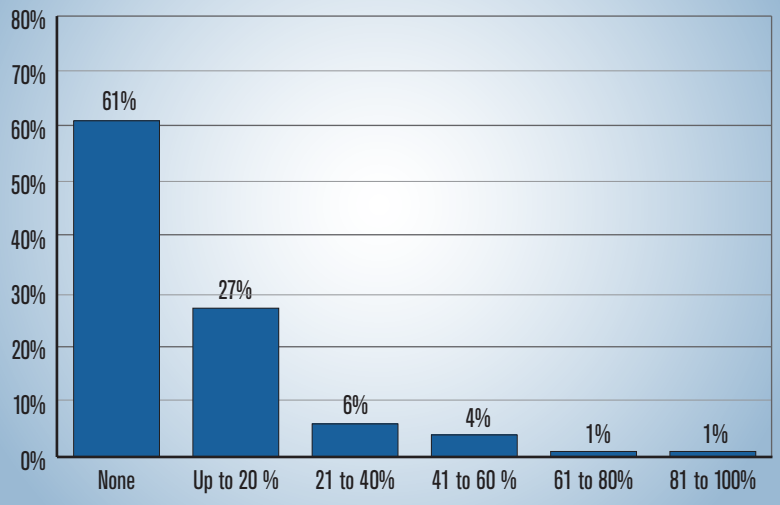


CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 512 Respondents

Figure 9. Percentage of Computer Security Functions Outsourced

By Percent of Respondents



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 609 Respondents

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 interpreted as agreeing with the statement. **Figure 8** illustrates that 42 percent of respondents indicate their organizations use ROI as a metric, 19 percent use NPV, and 21 percent use IRR. The popularity of these metrics is slightly up from the 38 percent, 18 percent, and 19 percent, respectively, reported in last year's findings. All three are down, however from the 55 percent, 25 percent, and 28 percent, respectively, reported in 2004, the first year the question was posed. Although ROI has a number of limitations when compared with NPV and IRR, ROI it is still by far the most popular metric used.[2]

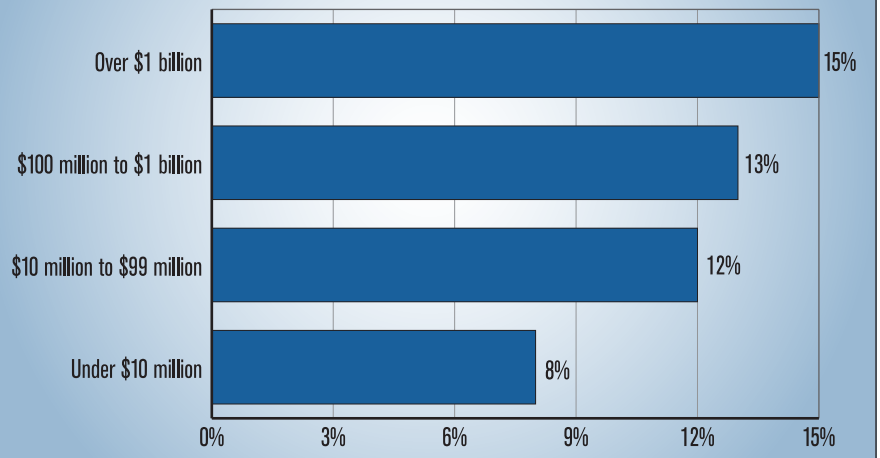
2. For a discussion of the limitations of ROI, see Lawrence A. Gordon and Martin P. Loeb, "Return on Information Security Investments: Myth vs. Reality," Strategic Finance, *November 2002, pp. 26–31.*

The 2004 survey saw the introduction of questions that dealt with outsourcing cybersecurity and the use of insurance as a tool for managing cybersecurity risks. While outsourcing continues to receive media attention, the 2006 survey shows that outsourcing of computer security work remains at approximately the same levels found in the previous two surveys. About one percent of respondents indicated that their organizations outsource more than 80 percent of the security function (**figure 9**, page 8). This year, 61 percent of respondents indicated that their organizations do no outsourcing of the security function as opposed to the 63 percent found in both the 2004 and 2005 surveys. If one accepts the almost universally held view that there continues to be an increase in IT outsourcing, then the results over the past three years indicate that managers view the security function differently from other IT work. **Figure 10** shows that, for firms that *do* outsource, the percentage of security outsourced increases with firm size. These percentages (8 percent for organizations with revenue under $10 million, 12 percent for those with revenue between $10 million and $99 million, 13 percent those with revenue between $100 million and $1 billion, and 15 percent those with revenue over $1 billion)

Figure 10. Average Percentage of Computer Security Functions Outsourced

(does not include the 61% of organizations that replied 'none' in figure 9)

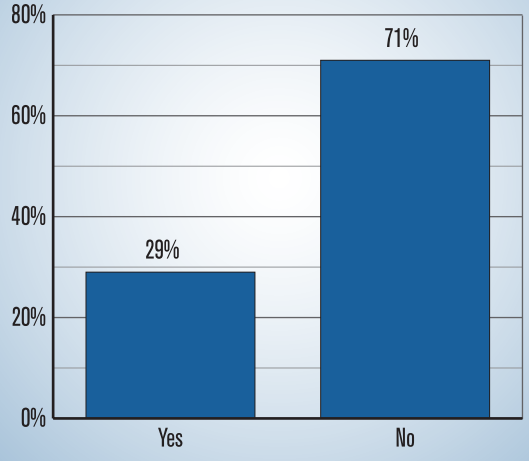
By Organization Revenue



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 609 Respondents

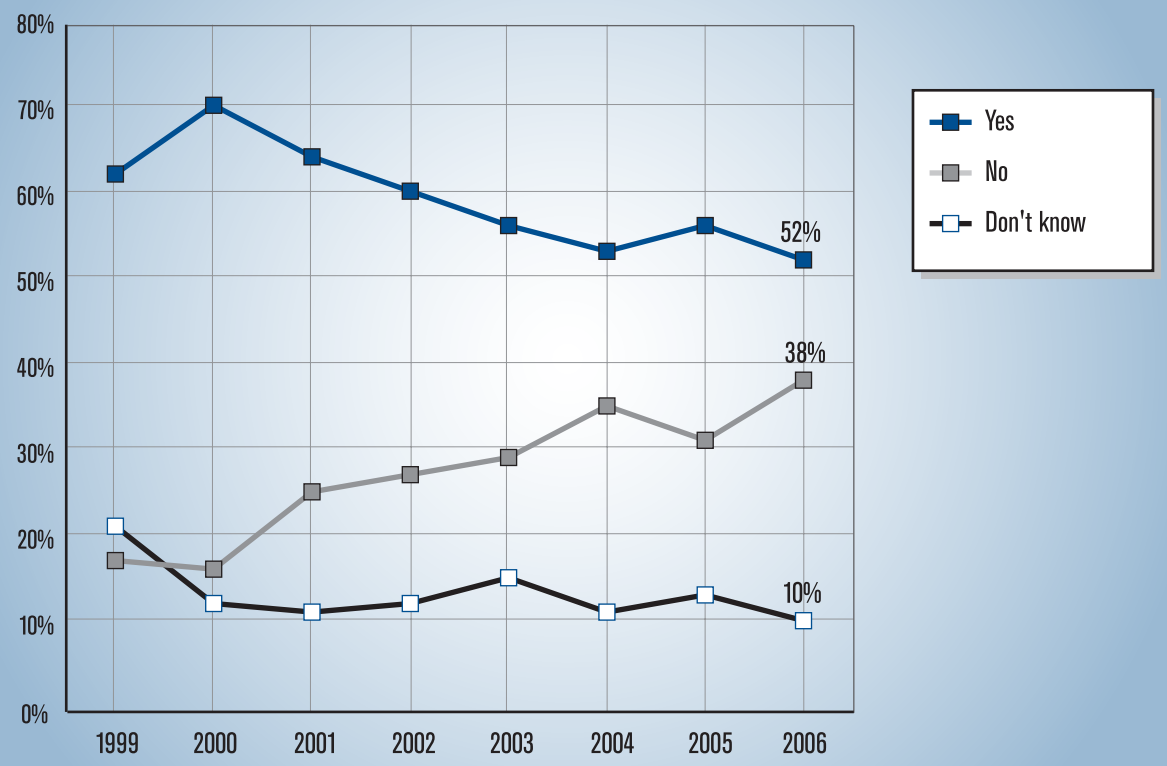
Figure 11. Does Your Firm Have Any External Insurance Policies to Manage Its Cybersecurity Risks?



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 571 Respondents

Figure 12. Unauthorized Use of Computer Systems Within the Last 12 Months



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

are considerably larger than the corresponding percentage found in last year's survey (4 percent, 8 percent, 7 percent and 9 percent, respectively). Finally, the survey also asked if the respondents would consider hiring a reformed hacker. An overwhelming majority of 606 respondents, 86 percent, answered that they would *not* consider hiring a reformed hacker.

Regardless of measures an organization may take to protect its systems using technical computer security measures such as the use of passwords, biometrics, antivirus software, and the like, there will be risks of financial loss that still remain. By purchasing cyber insurance, organizations are able to reduce these remaining risks. A number of companies do offer such policies, but because of the lack of good actuarial data on which to base insurance rates, providers have the incentive to add additional risk premiums to the prices they charge for these policies.[3] Over time one would expect that as insurance companies gain experience with this new product the additional risk premiums would shrink and prices for such policies would become more attractive. This, together with organizations becoming more familiar

3. For further analysis of the economics underlying cybersecurity insurance, along with examples of cyber insurance policies, see Lawrence A. Gordon, Martin P. Loeb and Tashfeen Sohail, "A Framework for Using Insurance for Cyber Risk Management," Communications of the ACM, *March 2003, pp. 81–85.*

with this new insurance product, would lead one to expect that the use of cyber insurance should be growing each year. As seen in **figure 11** (page 9), the percent of respondents in the 2006 survey that indicated that their organizations use cyber insurance is 29 percent. While the use of such cyber insurance remains low, the 29 percent figure is up from the 25 percent found in the 2005 survey. The general sense of the authors is that this in fact indicates a rising trend in the adoption of cyber insurance, but it's worth noting that 28 percent of respondents reported using cyber insurance in the 2004 survey, the first year this question was asked.

Table 1: How Many Incidents?

How many incidents, by % of respondents	1–5	6–10	>10	Don't know
2006	48	15	9	28
2005	43	19	9	28
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

CSI/FBI 2006 Computer Crime and Security Survey — 2006: 341 Respondents
Source: Computer Security Institute

Frequency, Nature and Cost of Cybersecurity Breaches

Figure 12 (page 10) shows that, after what appears to have been a slight pause last year, the decline of the overall frequency of successful attacks on computer systems resumed this year. The percentage of respondents answering that their organization experienced unauthorized use of computer systems in the last 12 months decreased slightly from 56 percent last year (and 53 percent the preceding year) to 52 percent this year. Furthermore, the percentage of respondents answering that there was no unauthorized use of their organization's computer systems increased from 31 percent (and 35 percent the prior year) to an all-time high of 38 percent this year. The percentage of respondents who indicated not knowing if such an unauthorized use occurred decreased from 13 percent to 10 percent, the lowest level in the history of the survey. The data reported in **table 1** also paint the picture of a slow decline in the frequency of attacks of computer systems. For firms reporting some incidents in the past year, the percentage of respondents reporting six or more attacks reached a new low (24 percent) in the survey's history, while the percentage of respondents reporting one to five attacks reached an all-time high (48 percent).

As noted in previous reports, "unauthorized use" is a broad category, covering undesired uses of computer and network resources in addition to abuses that are traditionally classified as "attacks." Trading offensive jokes among colleagues using a corporate e-mail server or storing downloaded music on an enterprise workstation in defiance of corporate policy would both constitute unauthorized use, but wouldn't be reflected in traditional cybercrime categories.

This year's questionnaire marked the move from a somewhat complex question that combined estimates of both source and frequency of attack to a new question that far more directly asked respondents to estimate attacks coming from inside an organization versus those from outside. **Figure 13** (page 12) shows the percentage of losses that respondents attributed to insiders. As can be seen in the figure, nearly one third (32 percent) of respondents believe that insider threats account for none of their organization's cyber losses. Another 29 percent of respondents attribute a percentage of losses greater than zero but less than 20 percent to actions of insiders. Hence, the remaining 39 percent of respondents attribute a percentage of their organization's losses greater

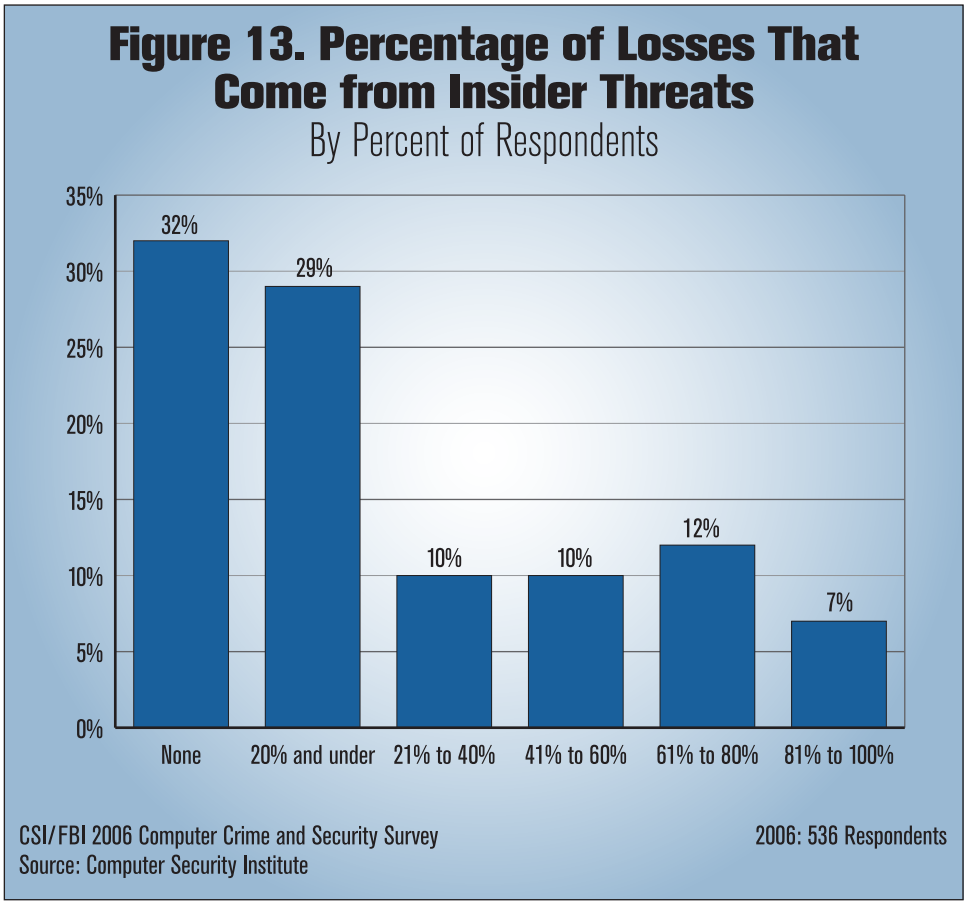
than 20 percent to insiders. In fact, 7 percent of respondents thought that insiders account for more than 80 percent of their organization's losses. To summarize, even though most respondents do not see insiders as accounting for most of their organization's cyber losses, a significant number of respondents believe that insiders still account for a substantial portion of losses.

For nearly all categories of attacks or misuse, **figure 14** (page 13) shows, the trend of such attacks detected appears to be decreasing over the years. However, there have been some small increases of reported attacks involving financial fraud, system penetration, sabotage, Web site defacement and misuse of public Web applications. Attacks involving unauthorized access to information and theft of proprietary information were reported at virtually the same levels as reported for 2005.

Last year's survey found that 95 percent of organizations reporting Web site incidents experienced more than 10 of such incidents. **Figure 15** (page 14) shows that for the 2006 survey, 59 percent experienced more than 10 such incidents. However, 36 percent of respondents that reported experiencing Web site incidents indicated that they were unable to specify the number. Hence, more than 92 percent (100(59/64)) of respondents who *were* able to specify the number of Web site incidents reported more than 10 of such incidents. Thus, defacement of Web sites continues to plague organizations.

Respondents' estimates of the losses caused by various types of computer security incident dropped significantly this year, as shown in **figure 16** (page 15). This is, in fact, the fourth consecutive year that these loss estimates have dropped. Indeed, while this year's decline is significant, it is the smallest *percentage* drop of the four years. Total losses for 2006 were $52,494,290 for the 313 respondents that were willing and able to estimate losses, down from the $130,104,542 losses for the 639 respondents that were willing and able to estimate losses in 2005. Much of the decrease in total losses is easily explained by the fact that the number of respondents willing to report their losses this year was less than half the number of the previous year. Nevertheless, there appears to have been a real decline, as the average loss per respondent decreased nearly 18 percent from $203,606 to $167,713.

Note that this decline in the average loss per respondent comes on top of last year's striking 61 percent decline from the $526,010 per respondent reported in the 2004 survey. Taking



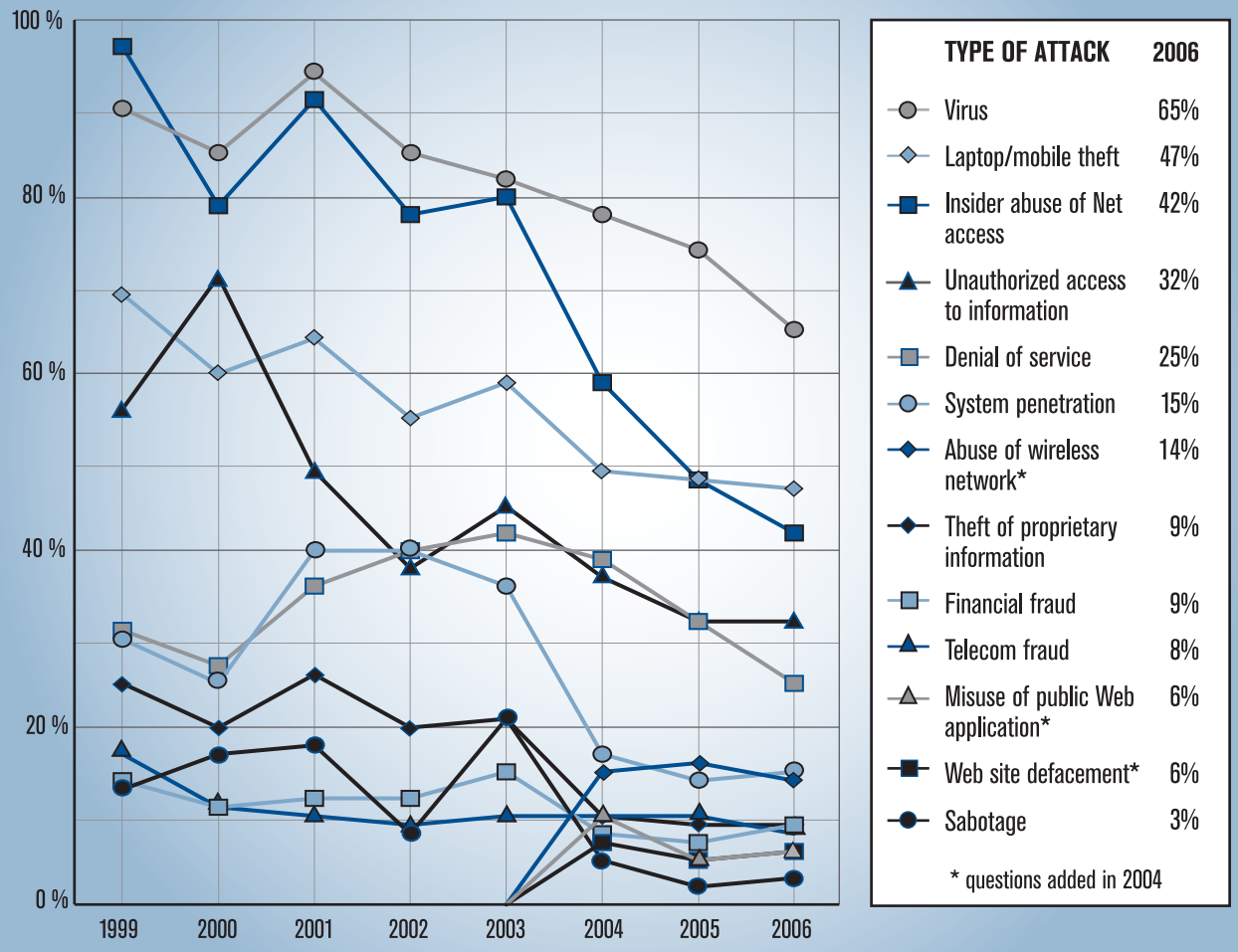
the last two years together, there was a decline in average losses of $358,297—a two-year decline of over 68 percent. Two factors we believe help to explain this decrease are the continued decline in reported incidents (see figure 14), and the dramatic increases in security investment by small and medium sized firms (see figures 6 and 7).

The top four categories of losses given in figure 16, (1) viruses, (2) unauthorized access, (3) laptop or mobile hardware theft and (4) theft of proprietary information, accounted for nearly three-quarters (74.3 percent) of the total losses.

Consistent with the overall decline in losses previously discussed and across nearly every type of loss, the average loss per respondent (based on the number of respondents reporting such a loss) declined. In fact, examples of categories of losses experiencing declines

Figure 14. Types of Attacks or Misuse Detected in the Last 12 Months

By Percent of Respondents



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

of average losses greater than 60 percent include unauthorized access to information (from $303,234 in 2005 to $85,621 in 2006), viruses (from $179,781 to $69,125) and denial of service category (from $56,672 to $20,872).

There were, however, three areas in which average losses *increased.* Losses from laptop or mobile hardware theft increased from $19,562 per respondent in 2005 to $30,057 per respondent in 2006. Losses from telecommunication fraud increased dramatically from $2,750 per respondent in 2005 to $12,377 per respondent in 2006. The third category in which average losses increased was Web site defacement. While the average losses for this category increased from $1,494 per respondent to $1,806 per respondent, less than one-third of a percent of total losses reported were due to Web site defacement.

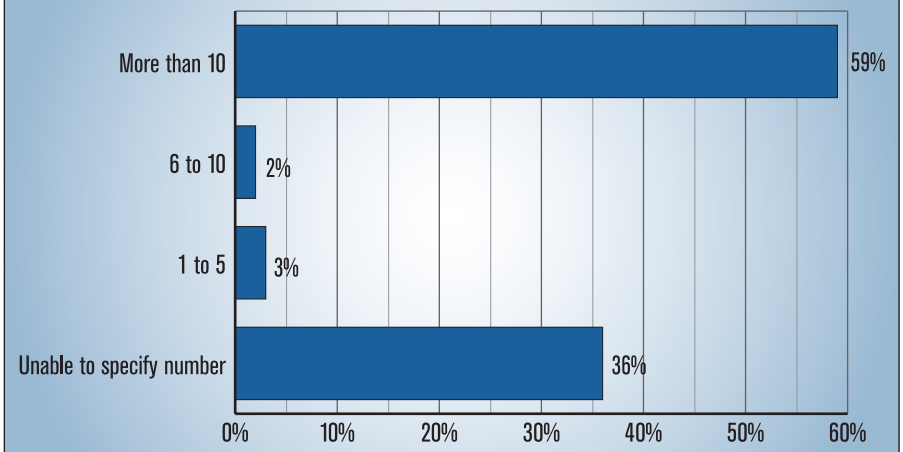
Increased security awareness and improved technology to cope with some threat types may account for much of the overall decline in reported losses. This may be particularly true for this survey pool, taken as it is from among the members of CSI. As noted in last year's report, the difficulty in interpreting overall downward trends is compounded by the difficulty of accurately measuring the implicit costs of losses associated with the theft of proprietary information and unauthorized access to information.

Respondents may be more accurate than ever in accounting for their explicit costs (lost productivity and the like). However, we are suspicious that *implicit* losses (such as the present value of future lost profits due to diminished reputation in the wake of negative media coverage following a breach) are largely not represented in the loss numbers reported here.

Security Technologies Used

As in previous years, respondents were asked to identify the types of security technology used by their organizations. This year's categories were expanded somewhat, but, the overall results given in **figure 17** (page 16) are approximately the same as last year. The new category of anti-spyware showed up as the third-most used security technology with 79 percent of respondents reporting its use. Use of firewalls was reported by 98 percent of respondents, and anti-virus software was reported by 97 percent. Server-based access control lists were used by 70 percent of the organizations and intrusion detection systems were being used by 69 percent of the organizations. While the reported use of biometrics is still small at 20 percent, its one-third increase in reported use from 15 percent in the 2005 survey is noteworthy. It will be interesting to see if the use of biometrics will continue to grow at a rapid rate in future years. There were only three other categories where similarly significant shifts were seen: namely encryption for data in transit and reusable account/login passwords (both down), along with IPS (which was up).

Figure 15. Percentage Experiencing Web Site Incidents



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

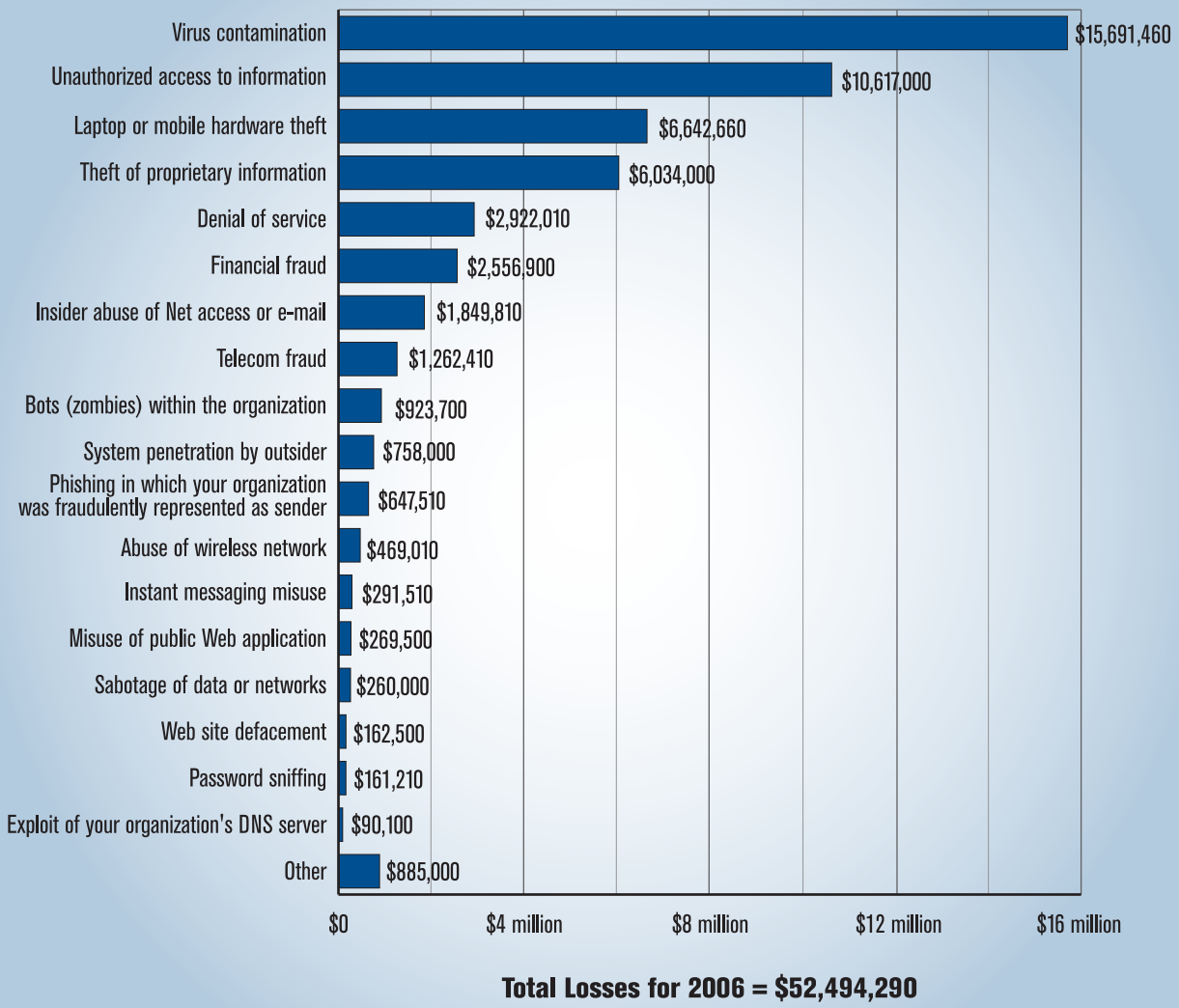
2006: 272 Respondents

One option that a solid majority of organizations opt *not* to employ in defending their networks is the employment of reformed hackers. On the seven-point scale measuring agreement and disagreement, the average response was a 2.4, indicating strong opposition to the notion. This is completely consistent with previous years when the question was posed.

Security Audits and Security Awareness Training

This year's questionnaire asked: "Which techniques does your organization use to assist in the evaluation of the effectiveness of its information security?" **Figure 18** (page 17) illustrates that 82 percent of respondents

Figure 16. Dollar Amount Losses by Type



Total Losses for 2006 = $52,494,290

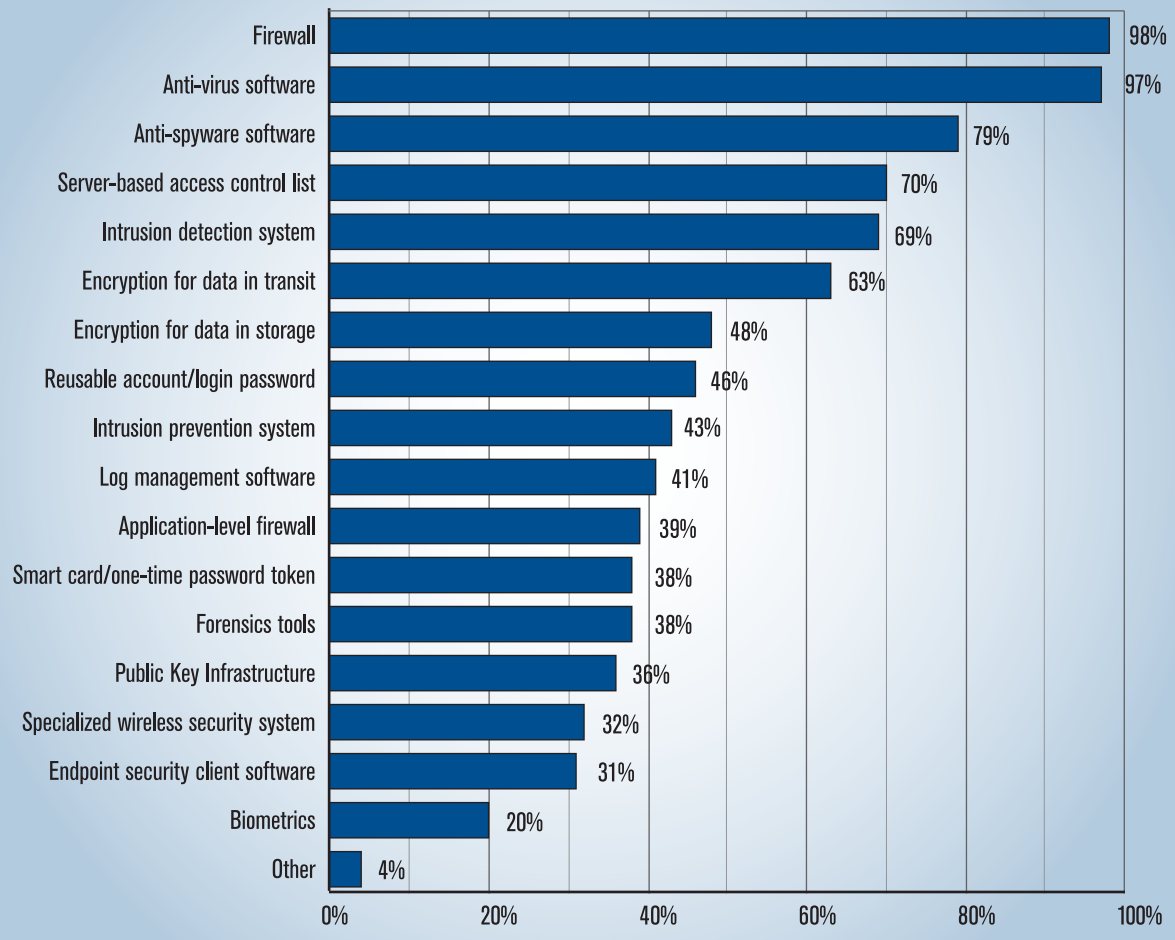
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 313 Respondents

report that their organizations use security audits conducted by their internal staff, making security audits the most popular technique in the evaluation of the effectiveness of information security. The 2005 survey reported the use of such security audits at 87 percent, while the prior year (the first year the security audit issue was addressed) also found use at 82 percent. Note that in these two prior years, the question did not distinguish between internal and external audits, so this year's 82 percent number isn't necessarily lower, given that it doesn't include external audits (which 62 percent of respondents reported using). Hence, use of security audits in a meaningful information security program appears to be holding at a high and fairly constant level. The use of the other techniques—penetration testing, automated tools, security audits by external organizations, e-mail monitoring software and Web activity monitoring software—are also widely used for

Figure 17. Security Technologies Used

By Percent of Respondents



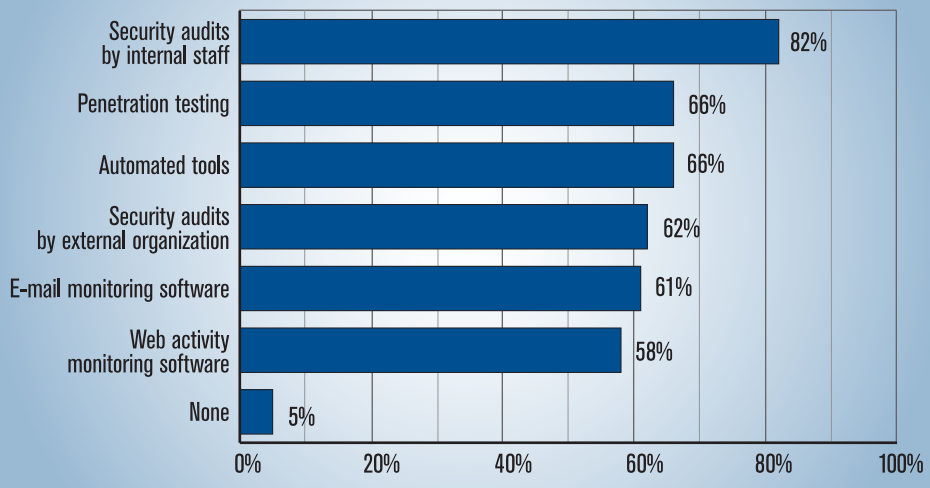
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

evaluation of the effectiveness of information security activities. These evaluation techniques are reported to be used by the organizations of 58 to 66 percent of the respondents.

For some time, it has been widely recognized that computer security is as much a management problem as it is a technology problem. Hence, technological responses to the problem must be combined with management responses. Thus, in addition to security audits, many organizations have invested in security training for their employees. Two questions addressing the extent and importance of security awareness training were first introduced in the 2004 survey. This year, respondents were asked to rate the degree to which they agreed with each of the three parts of the following statement, "My organization invests the appropriate amount on the following security related activities (1) operating expenditures, (2) capital investments, and (3) awareness training."

Figure 18. Techniques Used to Evaluate Effectiveness of Security



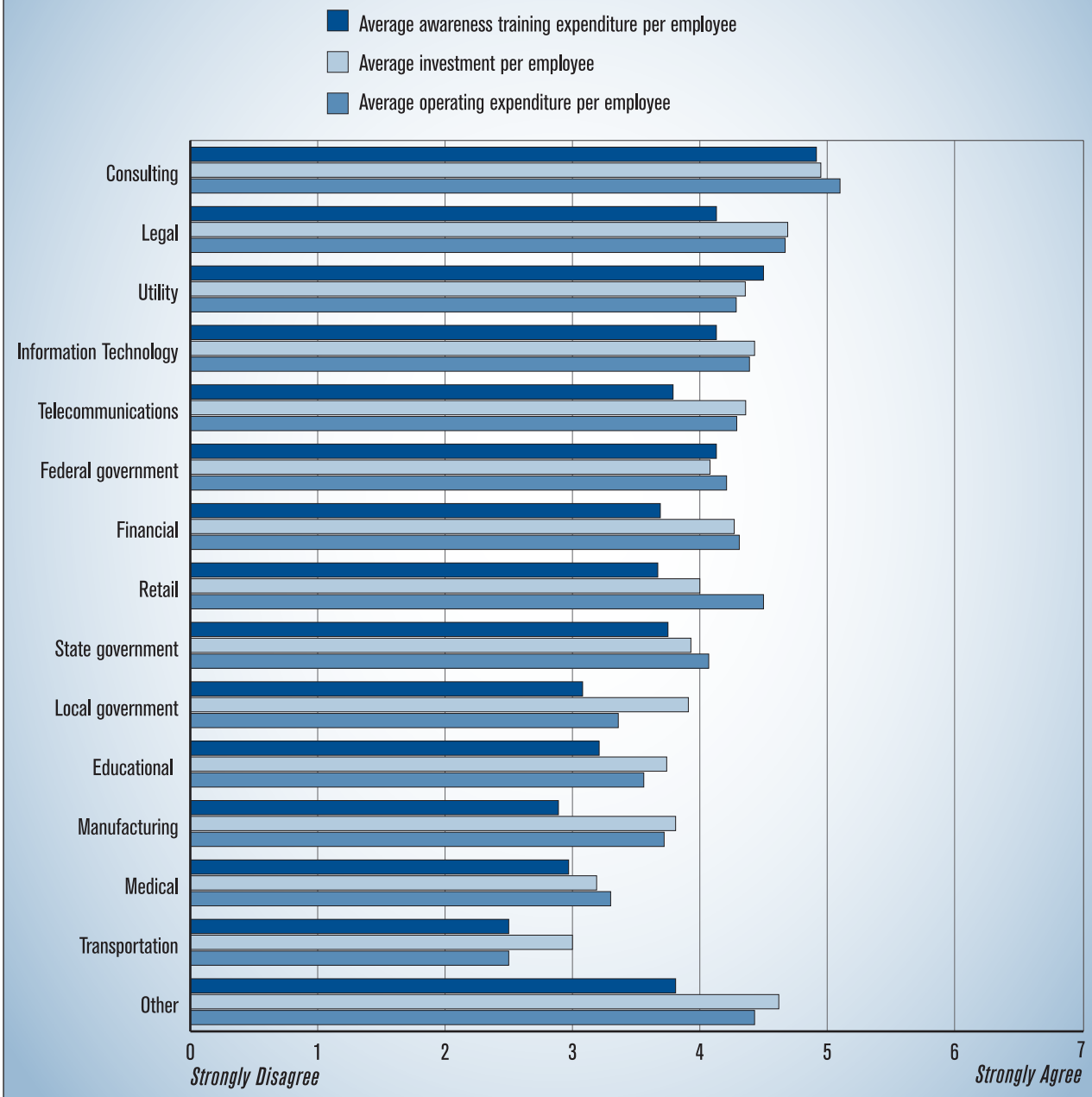
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute
2006: 597 Respondents

Figure 19 (page 18) illustrates that, on average, respondents from 10 out of 15 sectors do *not* believe that their organization invests enough in security awareness. The sectors in which respondents, on average, find sufficient investments in awareness training are consulting, legal, utility, information technology and federal government. The most notable changes—all shifts to a more benign view of resources devoted to awareness training—occurred in the legal and utility sectors. The perception that sufficient resources are being devoted to overall security-related operating expenditures and capital investments is generally much higher than for awareness training. From figure 19, one can see that in all but three sectors (federal government, utilities and transportation) respondents believe resources devoted to awareness training are less adequate than the resources devoted to either operating expenditures or capital expenditures. Thus, in the respondents' view, security awareness training appears to be a prime area for additional funding.

Survey participants were also asked to rate the importance of security awareness training to their organizations in each of several areas. **Figure 20** (page 20) shows the percentages of respondents indicating that awareness training was very important (as measured by importance ratings of 5 or above on seven-point scale) in the various areas of security. For seven of the eight security areas listed, the average rating indicated that training for that area was very important. Of the top five areas, security policy (77 percent), network security (76 percent), security management (72 percent), access control systems (67 percent) were also among the security areas identified by last year's respondents as an area in which security training is important. This year three

Figure 19. Organization Invests the Appropriate Amount on Security Operating Expenditures, Capital Investment and Awareness Training

Mean Values Reported on a Seven-Point Scale



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 483 Respondents

other areas were also identified by a majority of respondents as areas in which security training is important. These areas are security systems architecture (62 percent), economic aspects of computer security (55 percent) and investigations and legal issues (52 percent). Compared to the 2005 survey, a larger percentage of respondents ranked six of the eight areas as important for security awareness training. We believe the increasing complexity of enterprise information systems and information security systems is driving the respondents to recognize the importance of security systems architecture training. The responses indicate an overall substantial increase in respondents' perception of the importance of security awareness training.

Information Sharing

Over the last several years there have been many calls for increased sharing of information as a way of combating cyber attacks. For example, one key action point highlighted in the National Strategy for Securing Cyberspace released by President Bush in 2003 was the encouragement of private sector information sharing.[4] Hence, questions related to information sharing were added to the survey beginning in 2004.

Respondents were asked if their organizations belong to an information sharing organization, and the results are shown in **figure 21** (page 20). About 29 percent of respondents indicated that their organizations belong to INFRAGARD, 17 percent belong to an information sharing and analysis center (ISAC), and 10 percent to some other security sharing organization. The comparable percentages from the 2005 report showed 32 percent belonging to INFRAGARD, 19 percent belonging to an ISAC and 30 percent to some other security sharing organization. These figures would seem to indicate a decline in membership of information sharing organizations. However, 44 percent of the respondents indicated that their organizations do not belong to any information sharing organization compared to 46 percent in the 2005 survey. These figures can be reconciled by noting that organizations could belong to multiple sharing groups, and this was apparently the case for the organizations of many of the 2005 survey respondents. In any case, it is clear that there was no surge to join information sharing organizations.

Beyond inquiring about membership in information sharing organizations, respondents were asked whether they shared information on computer intrusions with law enforcement and legal counsel. **Figure 22** (page 21) shows how the organizations surveyed responded to computer intrusions in each year beginning with 1999. The top line shows that 70 percent of respondents indicated that their organization responds by patching security holes. This is the lowest level in the eight-year period covered in figure 22, and follows an even larger drop from 2004 to 2005 (from 91 percent to 73 percent). The continued drop may be due to improved, automated approaches for patch dissemination and installation, which makes that process transparent to most.

The next line down in the figure shows that 70 percent (100 percent - 30 percent) of all respondents indicated that their organization share information about a security breach. The percentage of respondents that did not report their computer intrusions reached the lowest level (30 percent) for the eight-year period. Hence, the notion of information sharing may finally be gaining traction. The third and fourth line down respectively in figure 23, show the percentage reporting to law enforcement (25 percent) and the percentage reporting to legal counsel (15 percent) reversed the multi-period lows reached last year, (20 percent and 12 percent, respectively).

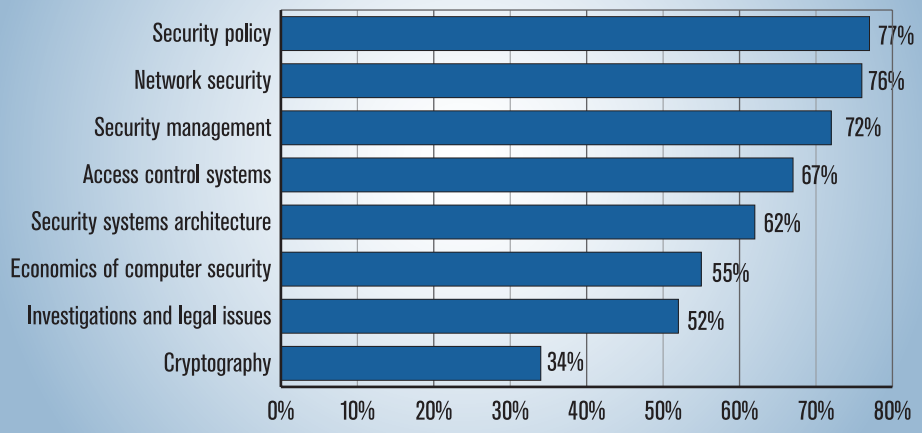
Figure 23 (page 22) summarizes the reasons why organizations did not report intrusions to law enforcement. This figure shows the percentages of respondents identifying each stated reason as being very important (as measured by an importance ratings of 5 or above on a seven-point scale) in the decision not to report the computer intrusion. The predominant reason given for not

4. See http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

reporting that was cited as being very important (by those indicating that their organizations would not report an intrusion to law enforcement) was the perception that resulting negative publicity would hurt their organization's stock and/or image.[5] This reason for not reporting is still the predominant reason given and increased from 43 percent to 48 percent over the last year. This year, 36 percent of respondents, as opposed to 33 percent last year, cited the advantage competitors could use as being very important. This year, there was a marked increase, from 16 percent last year to 27 percent, in the portion of respondents that indicated that using a civil remedy was a very important reason for not reporting the intrusion. The claim, that being unaware of law enforcement's interest in the breach, was cited by 22 percent (versus 16 percent last year) as a very important reason for failure to report the intrusion. Nonetheless, 78 percent of organizations *were* aware of law enforcement's interest and still choose not to report most computer crimes. Overall, the results concerning the willingness of organizations fully to participate

Figure 20. Importance of Security Awareness Training

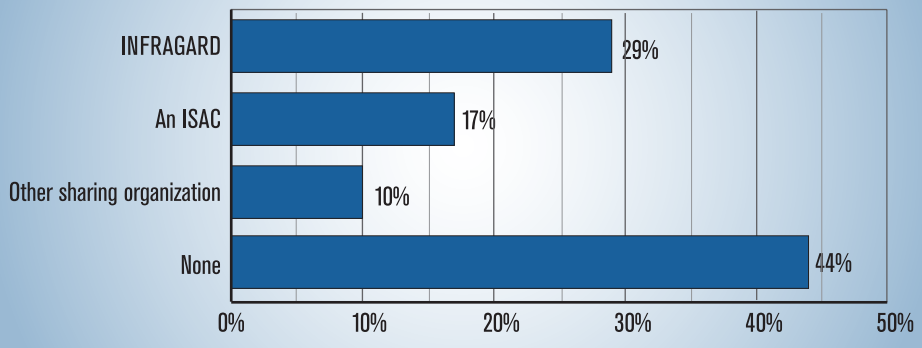
By Percent of Respondents Identifying as Important



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 599 Respondents

Figure 21. Percentage of Respondents That Belong to an Info Sharing Organization



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 606 Respondents

5. 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 stock's firm price.*

in information sharing of security breaches is consistent with recent theoretical work by three of the authors.[6]

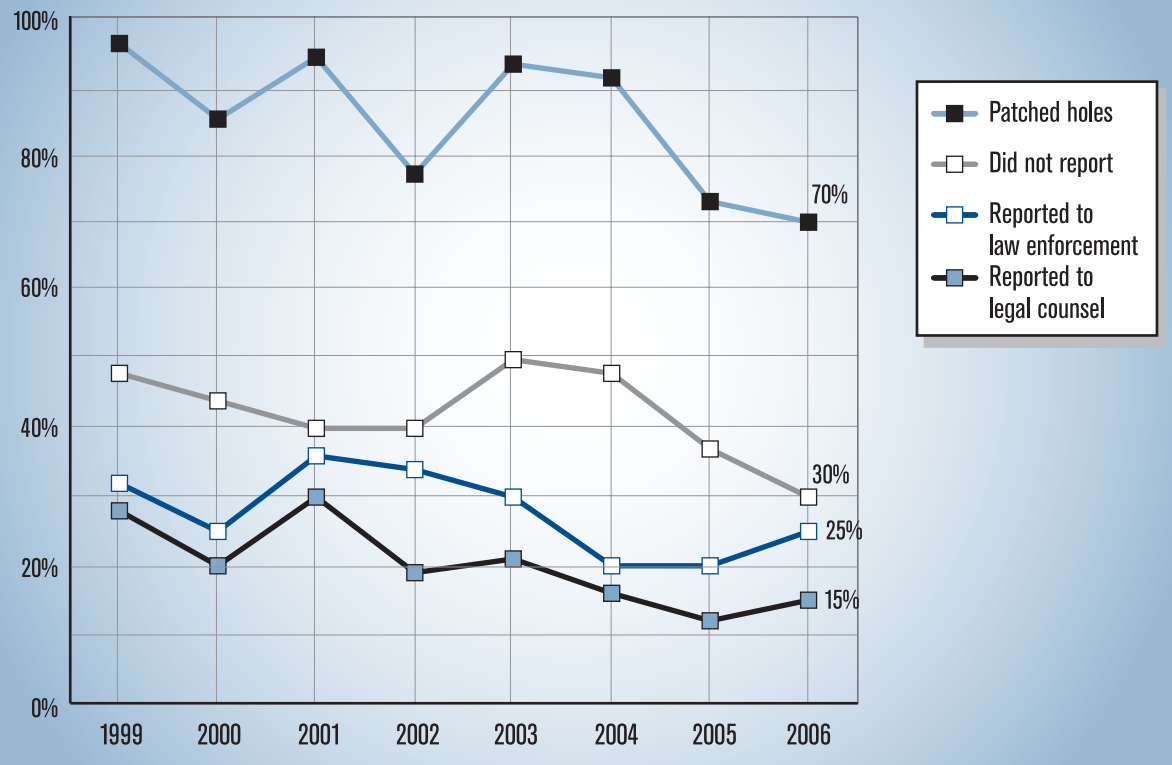
Effect of Sarbanes–Oxley Act

This year's questionnaire asked a question first introduced in 2004 to determine the effect, if any, of the Sarbanes–Oxley Act on the information security activities. As shown in **figure 24** (page 23), at least 50 percent of the respondents in seven out of 15 sector categories (telecommunications, retail, financial, manufacturing, information technology, consulting and other) agree with the statement "compliance with the Sarbanes–Oxley Act has raised my organization's level of interest in information security."[7] The corresponding figures in last year's survey showed eight out of the (then) 14 sectors with at least 50 percent agreement. This year, however, more than 60 percent of respondents in four of the

6. See Lawrence A. Gordon, Martin P. Loeb 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.*

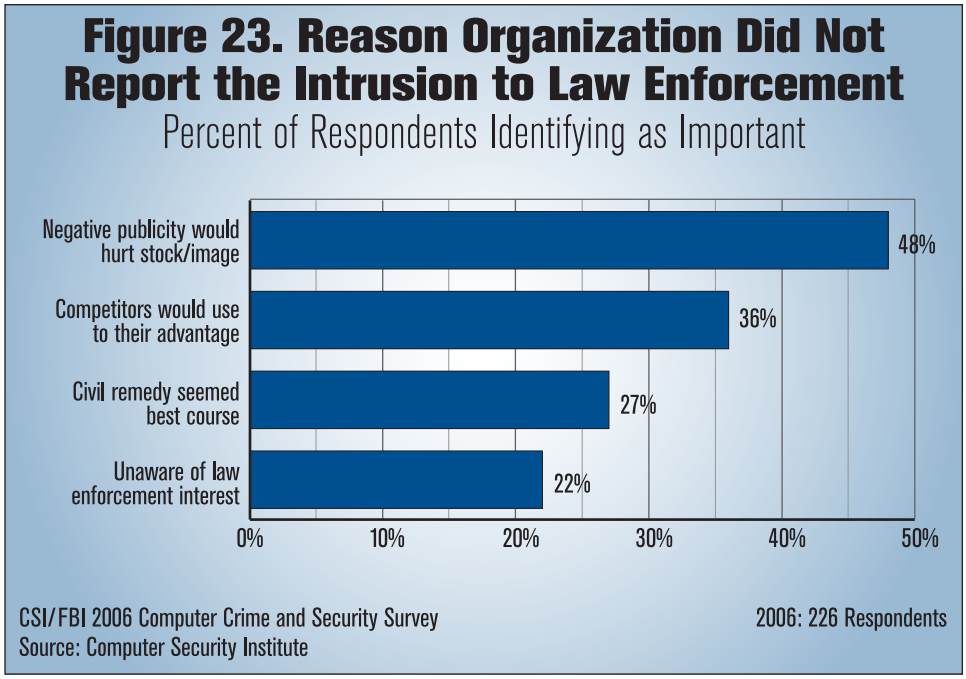
7. The new version of OMB Circular A-123—the implementing guidance for the Federal Managers Financial Integrity Act—requires agency heads to accept responsibility for, and annually assert to the effectiveness of their internal controls over financial reporting, similar to Section 404 of the Sarbanes–Oxley Act.

Figure 22. Actions Taken After Computer Intrusion(s) in the Last 12 Months



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 385 Respondents



sectors (telecommunications, retail, financial and manufacturing) agree that the Sarbanes–Oxley Act raised the level of interest in information security, while last year there were no sectors in which respondents reached 60 percent agreement.

Additionally, last year, respondents in only one sector had greater than 50 percent agreement with the statement "The Sarbanes–Oxley Act has changed the focus of information security in my organization from technology to one of corporate governance." This year more than 50 percent of respondents in three industries (telecommunication, retail and financial) agreed with that statement. Open-ended comments by respondents, discussed below, reinforce the conclusion that the Sarbanes–Oxley Act continues to change the information security landscape.

Finally, the 2006 survey also introduced the following open-ended question: "What do you think will be the most critical computer security issue(s) your organization will face over the next two years?" The responses of 426 respondents are categorized in **table 2** (page 24). As the table shows, the top five categories in terms of number of responses identifying the issue were (1) data protection, (2) regulatory compliance (including Sarbanes–Oxley), (3) identity theft and leakage of private information (4) viruses and worms, and (5) management involvement, risk management and resource allocation. Two categories tied for the fifth and sixth place and seventh place—access control and awareness training and other education initiatives.

Concluding Comments

The country's economy relies heavily on networked computer information systems for commerce, communications, energy distribution and transportation, as well as a host of other critical activities. The current momentum is clear—this dependence on computer-based, networked information systems will only increase. When services are interrupted and data stolen or misused, then property and even lives are placed at risk. At a more mundane level, cybercrime and the attendant threat of identity theft[8] reduce user and consumer confidence, slowing the acceptance of e-commerce. As a result, computer security, a critical activity that helps to protect these systems, has rightfully moved to a position of prominence in most organizations.

That does not mean, however, that those responsible for computer security get all the resources they want, or perhaps even all that they need. As highlighted in the survey, they have to make their case: security professionals are increasingly being asked to develop

8. A 2003 Federal Trade Commission identified about $48 billion in losses to institutions and an additional $5 billion in losses to individuals. Although not part of this CSI/FBI survey, the FTC findings help to explain the perception of losses much larger than the respondents indicated.

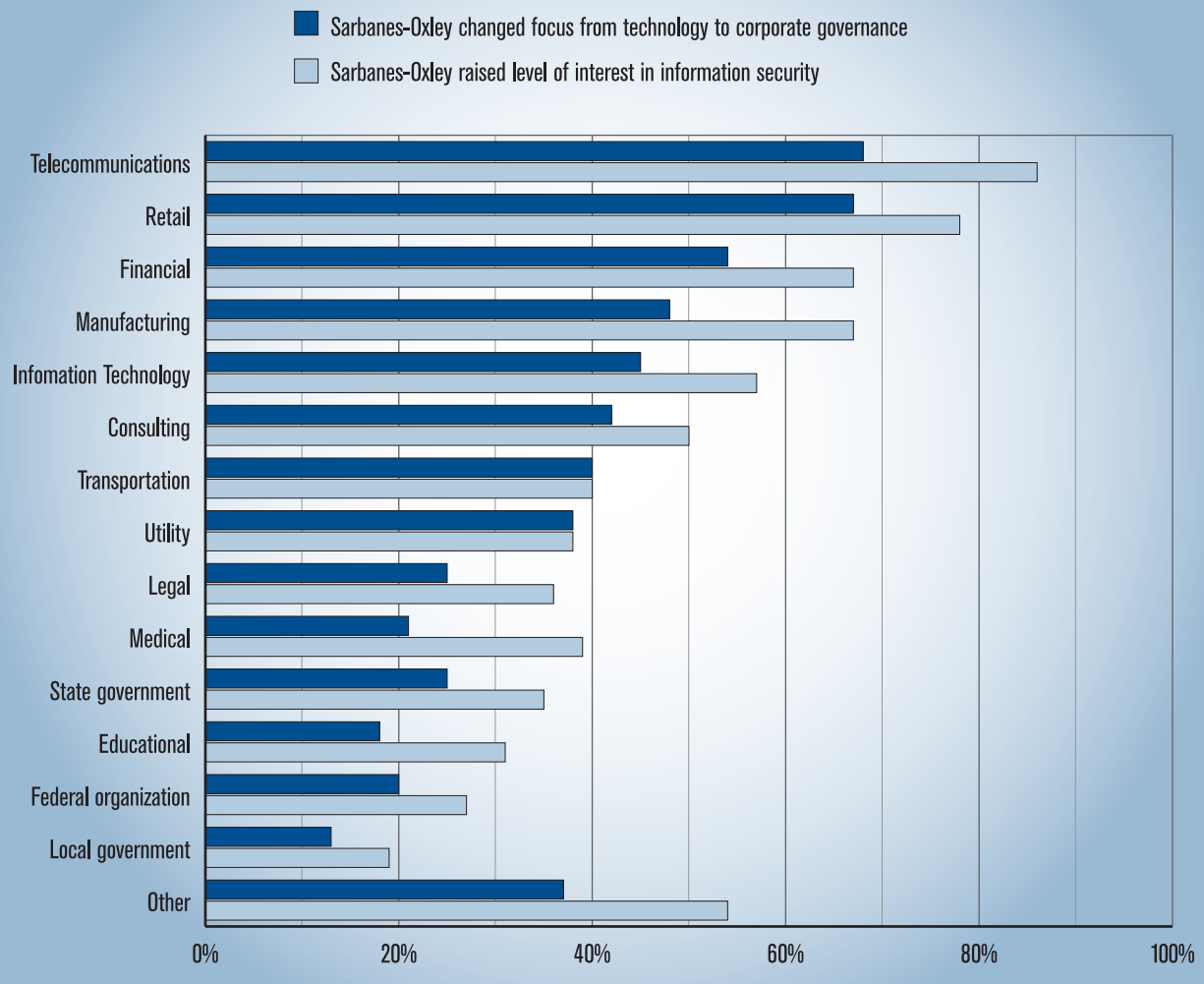
detailed business cases to justify new investments in technologies they need to address the constantly evolving threat. Therefore, in addition to being well versed with all the applicable technologies, computer security professionals must also understand the economic, financial, and risk management aspects of computer security.[9]

As with any other problem, the more knowledge we have about the causes and consequences, in this case of computer security breaches, as well as the way

9. Readers interested in a more detailed explanation on how to use economics/financial metrics in managing cybersecurity resources should see Managing Cybersecurity Resources: A Cost-Benefit Analysis, *by Lawrence A. Gordon and Martin P. Loeb (2006).*

Figure 24. Sarbanes-Oxley Act Has Made an Impact on Information Security

Percentage of Respondents that Agree



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 601 Respondents

Table 2. Respondents Identify the Most Critical Issues for the Next Two Years

Most critical computer security issues in next two years	# of respondents
Data protection (e.g.., data classiification, identification and encryption) and application software (e.g. Web application, VoIP) vulnerability security	73
Policy and regulatory compliance (Sarbanes-Oxley, HIPAA)	63
Identity theft and leakage of private information (e.g. proprietary information, intellectual property and business secrets)	58
Viruses and worms	52
Management involvement, risk management, or supportive resources (human resources, capital budgeting and expenditures)	47
Access control (e.g. passwords)	43
User education, training and awareness	43
Wireless infrastructure security	41
Internal network security (e.g. insider threat)	38
Spyware	34
Social engineering (e.g. phishing, pharming)	33
Mobile (handheld) computing devices	27
Malware or malicious code	20
Patch management	17
Zero-day attacks	16
Intrusion detection systems	16
Instant messaging	15
E-mail attacks (e.g. spam)	15
Employee misuse	12
Physical security	10
Web attacks	9
Two-factor authentication	9
Bots and botnets	7
Disaster recovery (e.g. data back-up)	7
Denial of service	7
Endpoint security	6
Managed cybersecurity provider	5
PKI implementation	4
Rootkits	3
Sniffing	3
Standardization, configuration management	3

CSI/FBI 2006 Computer Crime and Security Survey — 2006: 426 Respondents
Source: Computer Security Institute

organizations address computer security issues, the more likely it is that organizations will be able to improve their computer security. The survey results presented in this report represent what we hope to be valuable additions to this required knowledge base. Our objectives remain as always, namely to follow key trends in the information security arena and to identify changes in the landscape as they become visible. Future CSI/FBI surveys will continue to focus on these twin objectives.

A NOTE FROM CSI EDITORIAL DIRECTOR ROBERT RICHARDSON

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 Intrusion 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. I must 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.

The involvement of three academicians (their biographies are below, page 27) who specialize in the economics of information security continued for a third year. Both I and the entire CSI team thank the academic team of Gordon, Loeb and Lucyshyn.

Particular thanks go to Sara Peters, associate editor, who saved us from ourselves.

Regarding Methodology

The survey was distributed to 5,000 information security practitioners in the United States in early January 2006, both in a hardcopy, first-class mailing and in a Web e-mail distribution. Two subsequent mailings and e-mailings followed at approximately two-week intervals. Print surveys were returned by business-reply mail; both print and Web surveys were administered anonymously.

Regarding Use of Survey Statistics

CSI encourages most uses of the survey. For purely academic, non-profit classroom use, you may use the survey freely. If you are quoting the survey in a research paper, for instance, you are granted permission here and do not need to contact CSI. For other uses, there are three general requirements you must meet.

- ❑ First, you should limit any excerpts to a modest amount—if you are quoting more than 800 words or reproducing more than two figures, you need special permission.
- ❑ Second, you must of course give appropriate credit—you must say that the material you are excerpting came from the CSI/FBI Computer Crime and Security Survey and mention the year of the survey.
- ❑ Third, you may not profit directly from your use of the survey (you may, however, use survey statistics and the like as part of marketing and advertising programs or as small parts of larger books or similar works).
- ❑ Finally, when the published or broadly distributed work in which you are using the quotation appears, you must agree to send a copy of the work, link to the work online, or clear indication of how the material was used to CSI at the contact addresses below (page 27). You are *not* granted permission to use any part of the survey if you do not agree to this provision—an important part of the service we try to provide with the annual survey involves knowing how the survey is used.

If you can meet these four requirements, you are hereby given permission to use the survey. If not, you should seek additional special permission.

Opinions offered in this report are those of the authors, and not necessarily those of the Federal Bureau of Investigation, the 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). Gordon and Loeb are also affiliate professors at the University of Maryland Institute for Advanced Computer Studies (UMIACS). WILLIAM LUCYSHYN is a Senior Research Scholar and the Director of Research of the Center for Public Policy and Private Enterprise in the School of Public Affairs at the University of Maryland (Lucyshyn@umd.edu), and ROBERT RICHARDSON is Editorial Director at the Computer Security Institute (rrichardson@cmp.com).

Contact Information

For referrals on specific criminal investigations:
Shena Boswell Crowe, Special Agent
San Francisco FBI Computer Crime Squad
(415) 553-7400
Shena.Crowe@ic.fbi.gov, subject line: CSI Report
For general information: NJPC.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 cybercrime is a critical concern. 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 33 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 415-947-6135
Toll-free 888-234-9476
Fax 415-947-6023
E-mail csi@cmp.com

GoCSI.com

Events and Training:

33rd Annual Computer Security Conference & Exhibition
November 6–8, 2006
Gaylord Palms Resort
Orlando, FL
The world's largest conference devoted to computer and information security

NetSec 2007
June 11–13, 2007
The Phoenician Resort
Scottsdale, AZ
A balanced perspective of managerial and technical issues makes this the most popular conference devoted to network security.

34th Annual Computer Security Conference & Exhibition
October 15–17, 2007
Gaylord Palms Resort
Orlando, FL

Two-Day Training Classes on Topics that Include:

- Awareness
- Risk Analysis
- Policies
- Forensics
- Intrusion Prevention
- Wireless Security
- Introduction to Computer Security

CSI/FBI Computer Crime and Security Survey Presentations:

September 12, 2006
Washington, D.C.

September 13, 2006
Boston

September 14, 2006
New York

September 26, 2006
Chicago

September 27, 2006
Los Angeles

September 28, 2006
San Francisco

Awareness:

FrontLine* and *TopLine
Awareness newsletters

Awareness Peer Groups

"World Security Challenge"
Online awareness training tool

CSI Member Benefits:

- Monthly Computer Security *Alert*
- Quarterly *Computer Security Journal*
- CSI member-only archives
- Discounts on conferences, training and publications
- Networking opportunities, career advancement and more

Not a CSI member? To start receiving the *Alert,* *Computer Security Journal* and other Membership benefits, go to **GoCSI.com** or call 800-250-2429.

CSI
COMPUTER SECURITY INSTITUTE