2005

CSI/FBI

COMPUTER CRIME AND SECURITY SURVEY

CSI

COMPUTER
SECURITY
INSTITUTE

Publications

GoCSI.com

2005

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 (CSI) with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The survey is now in its 10th 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 700 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities.

The 2005 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 in the survey include:

❑ Unauthorized use of computer systems.
❑ The number of incidents from outside, as well as inside, an organization.
❑ Types of attacks or misuse detected.
❑ 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. In this regard, some perspective is now gained on the below new issues that were introduced in last year's 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:

❑ How organizations evaluate the performance of their investments in computer security.
❑ The security training needs of organizations.
❑ The level of organizational spending on security investments.
❑ The impact of outsourcing on computer security activities.
❑ The role of the Sarbanes-Oxley Act of 2002 on security activities.
❑ The use of security audits and external insurance.
❑ The portion of the IT (information technology) budget organizations devote to computer security.

KEY FINDINGS

Prior to highlighting some key findings of this year's survey, one should note that the number of responses increased dramatically this year. The responses went from 494 responses in 2004 to 700 responses in 2005, even though the sample size remained the same. This was likely due in some measure to an increase in the number of reminders sent to the sample group. See the end note regarding methodology for further details (page 23).

Some key findings:

❏ Virus attacks continue as the source of the greatest financial losses. Unauthorized access, however, showed a dramatic cost increase and replaced denial of service as the second most significant contributor to computer crime losses during the past year.

❏ Unauthorized use of computer systems has increased slightly according to the respondents. However, the survey respondents reported that the total dollar amount of financial losses resulting from cybercrime is decreasing. Given that the total number of respondents to the survey has dramatically increased, the survey shows a dramatic decrease in average total losses per respondent. Two specific areas (unauthorized access to information and theft of proprietary information) did show significant increases in average loss per respondent.

❏ Web site incidents have increased dramatically.

❏ State governments currently have both the largest information security operating expense and investment per employee of all industry/government segments.

❏ Despite talk of increasing outsourcing, the survey results related to outsourcing are nearly identical to those reported last year and indicate very little outsourcing of information security activities. Among those organizations that do outsource some computer security activities, the percentage of activities outsourced is quite low.

❏ Use of cyber insurance remains low (i.e., cyber-security insurance is not catching on despite the numerous articles that now discuss the emerging role of cybersecurity insurance).

❏ The percentage of organizations reporting computer intrusions to law enforcement has continued its multi-year decline. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity.

❏ A significant number of organizations conduct some form of economic evaluation of their security expenditures, with 38 percent using Return on Investment (ROI), 19 percent using Internal Rate of Return (IRR) and 18 percent using Net Present Value (NPV).

❏ Over 87 percent of the organizations conduct security audits, up from 82 percent in last year's survey.

❏ The Sarbanes-Oxley Act has begun to have an impact on information security in more industry sectors than last year.

❏ The vast majority of respondents view security awareness training as important. However, (on average) respondents from all sectors do not believe their organization invests enough in it.

DETAILED SURVEY RESULTS

NOTE: Dates on the figures refer to the year of the report (i.e., 2005). The supporting data is based on the 2004 calendar year.

About the Respondents

Figures 1 through 4 summarize information about the organizations that responded to this year's survey, and the individuals representing those organizations. Generally speaking, the demographics of survey respondents have remained roughly consistent over the past several years, making it reasonable to draw some conclusions regarding trends in the year-over-year data. Because the survey is based on anonymous responses, it's not possible to perform direct longitudinal analyses that might more definitively support these conclusions.

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 the financial sector (17 percent), followed by high-tech (15 percent) and manufacturing (9 percent). The government agency portion (combining federal, state and local levels) was 16 percent and educational institutions accounted for 6 percent of the responses. The diversity of organizations was also reflected in the large portion (19 percent) designated as "Other." The proportion of respondents coming from the various sectors remains roughly the same as in previous years.

The size of the organizations, as measured by number of employees, that are represented in the survey can be seen in figure 2 (page 4). Organizations with more than 1,500 employees accounted for half of the responses. The single largest size category of organizations responding was the category having from 1,500 to 9,999 employees. This group accounted for 23 percent of all responses. The category covering the largest organizations—those with 50,000 or more employees—made up 11 percent of all responses. As in the past, a substantial minority of responses (20 percent this year, compared to 19 percent last year) came from firms having fewer than 100 employees.
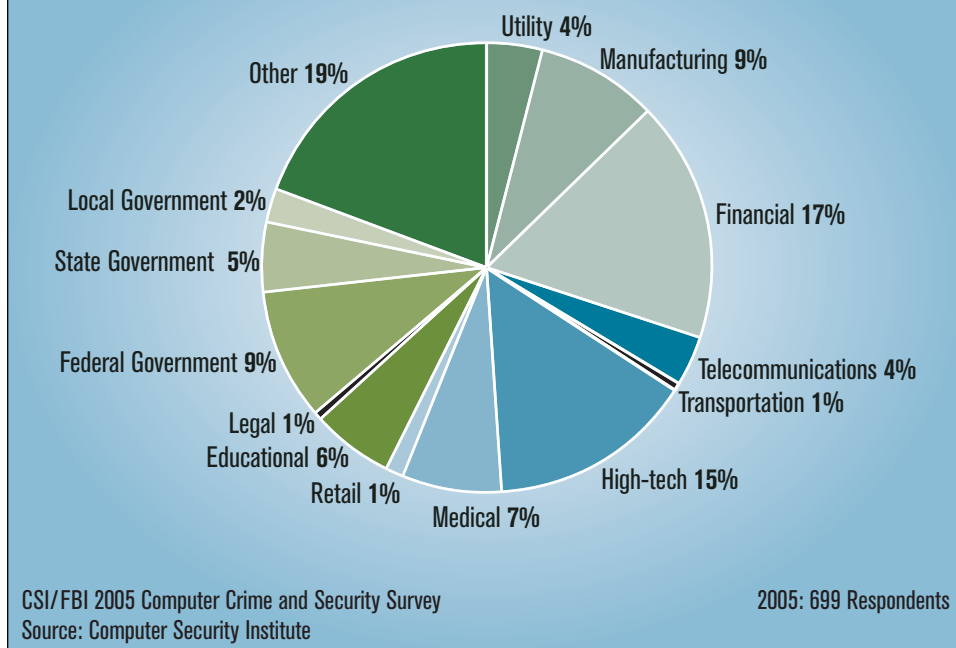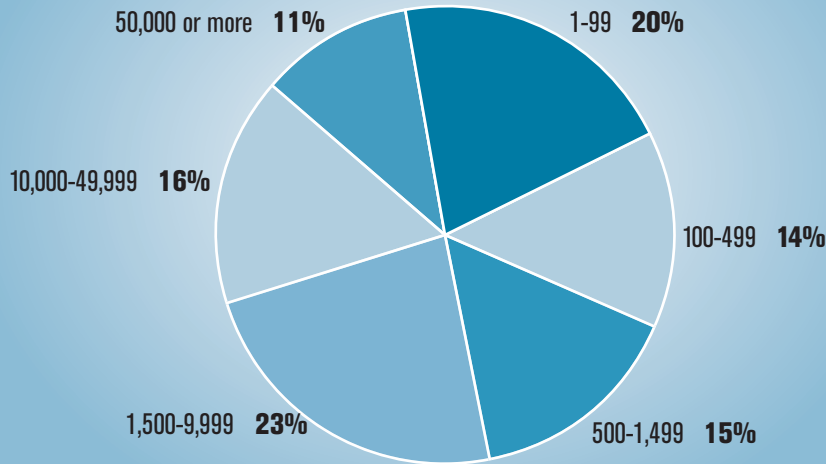

Figure 1. Respondents by Industry Sector

Utility 4%
Manufacturing 9%
Other 19%
Financial 17%
Local Government 2%
State Government 5%
Telecommunications 4%
Transportation 1%
Federal Government 9%
Legal 1%
Educational 6%
Retail 1%
Medical 7%
High-tech 15%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 699 Respondents

Figure 2. Respondents by Number of Employees
(Numbers do not total 100% due to rounding.)

50,000 or more **11%**

1-99 **20%**

10,000-49,999 **16%**

100-499 **14%**

500-1,499 **15%**

1,500-9,999 **23%**

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 699 Respondents

Figure 3. Respondents by Revenue

Over $1 billion **37%**

Under $10 million **25%**

$10 million to $99 million **18%**
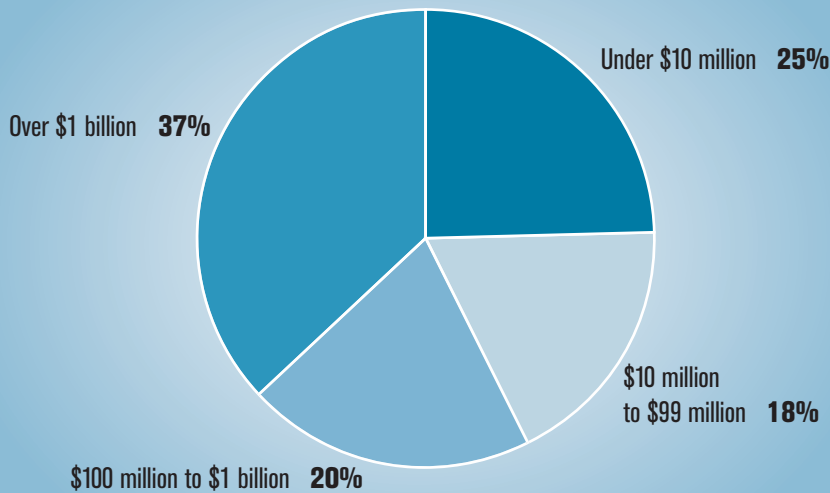
$100 million to $1 billion **20%**

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 549 Respondents

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 $100 million, including 37 percent generating annual revenues in excess of $1 billion, the largest firms in America are well-represented in our survey findings. Nevertheless, 25 percent of the responding firms generated annual revenues under $10 million. Comparing these numbers with earlier CSI/FBI Computer Crime and Security Surveys, one sees that roughly the same size firms responded over time—again allowing us to make some meaningful trend analyses.

For the second consecutive year, the survey sought to categorize respondents by job title. Figure 4 (page 5) illustrates that 32 percent of the respondents were senior executives with the titles of chief executive officer (CEO) (8 percent), chief information officer (CIO) (6 percent), chief security officer (CSO) (5 percent) or chief information

security officer (CISO) (13 percent). The single largest category of respondents (26 percent) had job titles of security officer, security manager, or security director. An additional 7 percent of respondents had the title of systems administrator, while 35 percent had various other titles. While nearly all respondents have crucial information security management responsibilities, the striking growth in the "Other" category from last year's 19 percent to 35 percent reflects the great diversity in titles resulting as more organizations add information security positions to their staff.

One final point worth considering with regard to the survey pool: respondents are all members of (or, in smaller numbers, conference attendees of) the Computer Security Institute. In other words, they are *trying* to be more secure. They are individuals who have shown an above-average interest in information security. It is probably reasonable to assume, thus, that they are more "security savvy" than a survey pool drawn from a broader cross section of information technology professionals.
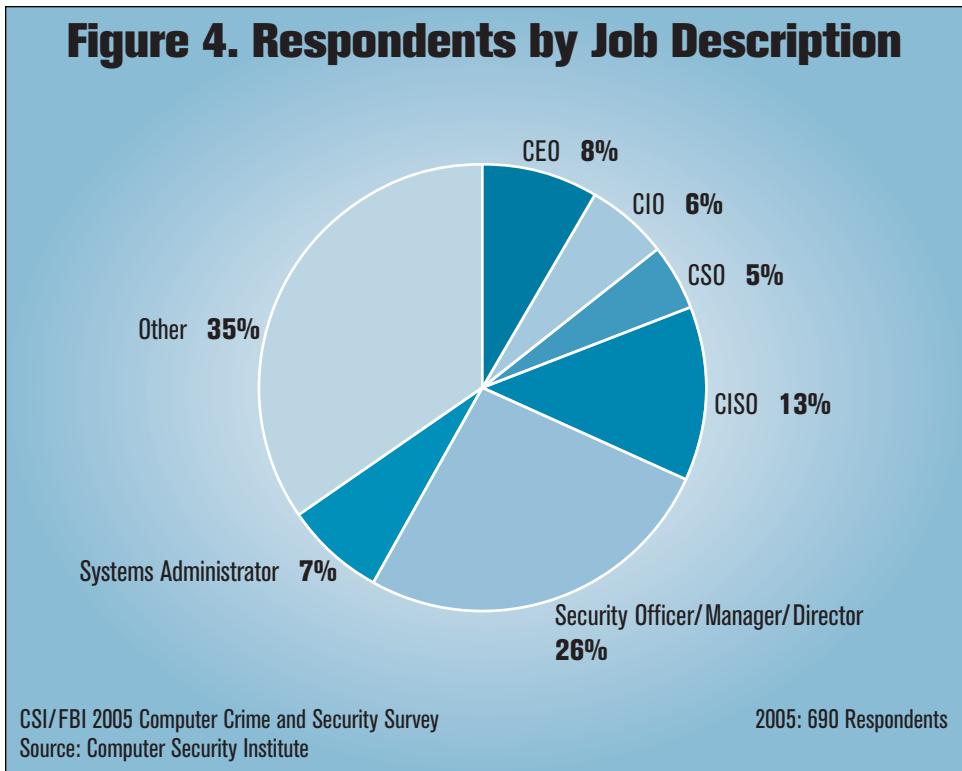
Figure 4. Respondents by Job Description

CEO **8%**
CIO **6%**
CSO **5%**
CISO **13%**
Security Officer/Manager/Director **26%**
Systems Administrator **7%**
Other **35%**

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 690 Respondents

Figure 5. Percentage of IT Budget Spent on Security
(Numbers do not total 100% due to rounding.)

Category	Percentage
More than 10%	8%
8-10%	11%
6-7%	8%
3-5%	24%
1-2%	24%
Less than 1%	11%
Unknown	15%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 690 Respondents

2005 CSI/FBI Computer Crime and Security Survey

Figure 6. Average Reported Computer Security Expenditure per Employee
By Organization Revenue

- Under $10 million: $358 (Average operating expense per employee), $285 (Average capital expenditure per employee)
- $10 million to $99 million: $89, $52
- $100 million to $1 billion: $216, $109
- Over $1 billion: $170, $77

Legend:
- ■ Average operating expense per employee
- ■ Average capital expenditure per employee

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 405 Respondents

Budgeting Issues

Information security managers seem to be well-aware that the financial and management aspects of dealing with security are as critical to their missions as are the technical aspects of security. While CSI/FBI surveys have always contained a number of questions related to the costs associated with information security breaches, the 2004 survey was redesigned to further explore a number of issues related to budgeting and financial management of information security risk. These design innovations were continued with the 2005 survey.

One question introduced a year ago 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 (page 5), 48 percent of respondents indicated that their organization allocated between 1 percent and 5 percent of the total IT budget to security. Only 11 percent of respondents indicated that security received less than 1 percent of the IT budget, 27 percent of respondents indicated that security received more that 5 percent of the budget, while 15 percent of the respondents indicated that the portion was unknown to them. A comparison with the 2004 results shows that there is essentially no change in the percentage of the IT budget allocated to security.

Another question added last year and maintained in the 2005 survey examined the average reported computer security operating expense and investment per employee. The 2004 results suggested that as a firm grows, computer security operating and capital

expenditures grow less rapidly (i.e., there are strictly increasing economies of scale when it comes to information security).

In contrast, the 2005 results, shown in figure 6 (page 6), tell a more complicated story. In particular, firms with annual sales under $10 million spent an average of approximately $643 per employee ($358 in operating expense and $285 in capital expenditures) on computer security; firms with annual sales between $10 million and $99 million spent an average of approximately $141 per employee ($89 in operating expense and $52 in capital expenditures) on computer security, and; firms with annual sales between $100 million and $1 billion spent an average of approximately $325 per employee ($216 in operating expense and $109 in capital expenditures) on computer security. The largest firms—those with annual sales over $1 billion—spent an average of about $247 per employee ($170 in operating expense and $77 in capital expenditures).

As indicated in figure 7, there were apparently some increasing returns to scale, since the smallest firms report computer security expenditures per employee substantially higher than all other categories.
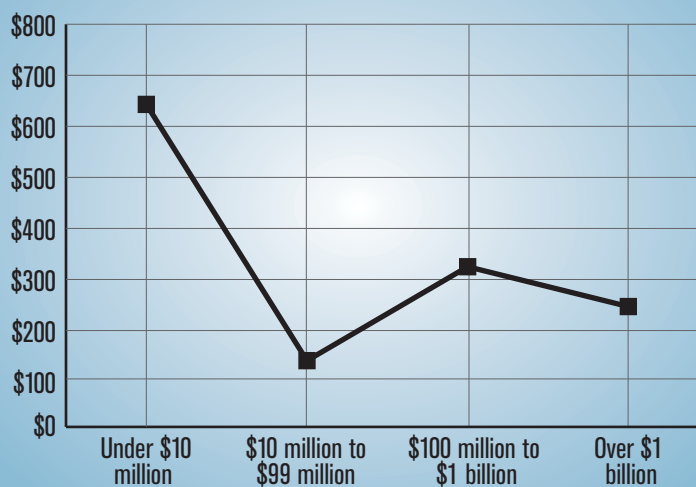
This year's finding makes a lot of economic sense, given that there is initially a large fixed investment for firms to ante up in terms of security. This fixed investment gets spread over a much larger number of employees as firms become larger, thereby reducing the average investment per employee. However, beyond some point, economies of scale caused by the fixed

portion of computer security expenditures diminish.

Spending per employee on computer security is shown again in figure 8 (page 8), broken down by sector for both private and public sector organizations. The highest average computer security spending per employee ($497) was reported by state governments ($354 of operating expenditures per employee and $143 of capital expenditures per employee). In terms of the operating expenditures on computer security per employee, the next highest sectors in descending order are utilities ($190), transportation ($187) and telecommunications ($132). In terms of the capital expenditures on computer security per employee, the next highest sectors in descending order were telecommunications ($72), utility ($62), followed by high-tech ($41).

The most noticeable changes from last year are seen in the federal and state government categories. Last year the federal government reported among the highest computer security spending per employee and state government was in the midrange of respondents.
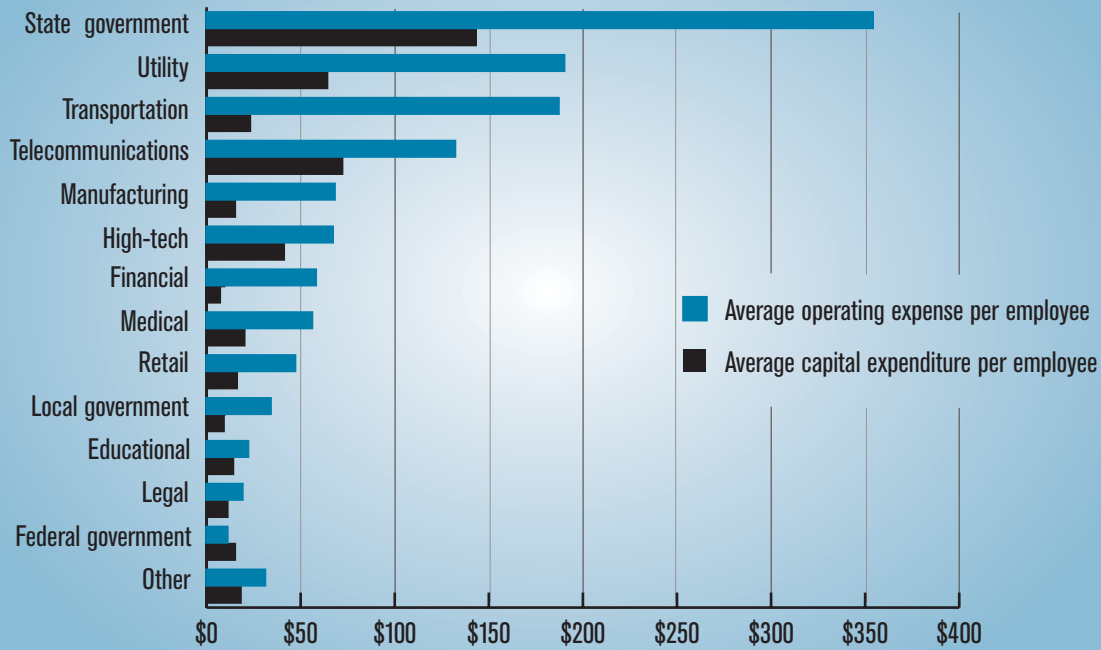

Figure 7. Average Reported Computer Security Expenditure per Employee
By Organization Revenue

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 405 Respondents

Figure 8. Average Reported Computer Security Expenditure/Investment per Employee
By Industry Sector

- Average operating expense per employee
- Average capital expenditure per employee

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 405 Respondents

This year, federal government respondents report among the least ($30 per employee composed of $19 per employee for operating expenditures and $11 per employee for capital expenditures) and state government security professionals are reporting the largest operating expenditures and capital investments per employee ($497 composed of $354 of operating expenditures and about $143 of capital expenditures per employee). One possible explanation for the large average employee expenditures by state governments is the plethora of state laws concerning information security that have been passed over the preceding few years.[1]

Managers responsible for computer security are increasingly required to justify their budget requests in purely economic terms. There has been considerable discussion of economic metrics used to justify and evaluate investments in computer security at trade and academic meetings, as well as in computer security journals. Therefore, beginning last year, the CSI/FBI Survey included a 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 costs and benefits of computer security expenditures.

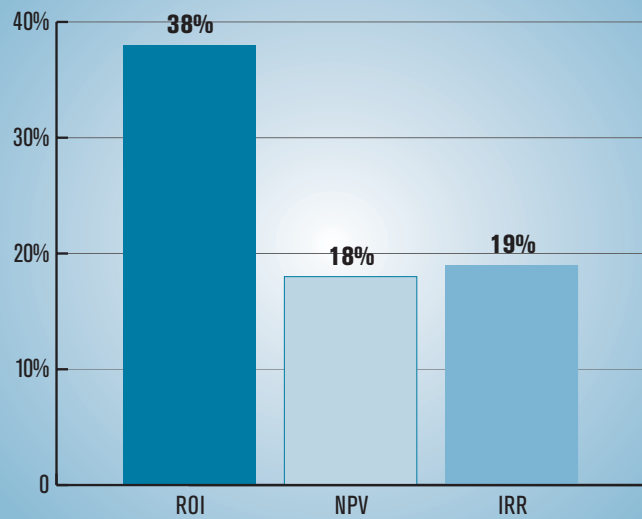In particular, survey participants were asked to

1. See Kurtz 2005 for an interesting discussion of the numerous state laws concerning information security recently enacted (http://www.virtualmgmt.com/csia/news/may_execdir.html).

indicate on a seven-point scale whether they agree or disagree that their organization uses ROI, NPV, or 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 9 illustrates that 38 percent of respondents indicate their organizations use ROI as a metric, 18 percent use NPV and 19 percent use IRR. Although the percentages seem significant, they are down from 55 percent, 28 percent, and 25 percent, respectively, reported in last year's findings. Although ROI has a number of limitations, when compared with NPV and IRR, ROI is still by far the most popular metric used.[2]

The widespread publicity associated with big name information security breaches over the past year may have resulted in information security investments being viewed as "must-do" projects not subject to stringent economic analysis. This would account for the decline in the use of all financial metrics during the past year. There is also some possibility that increasing

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.*

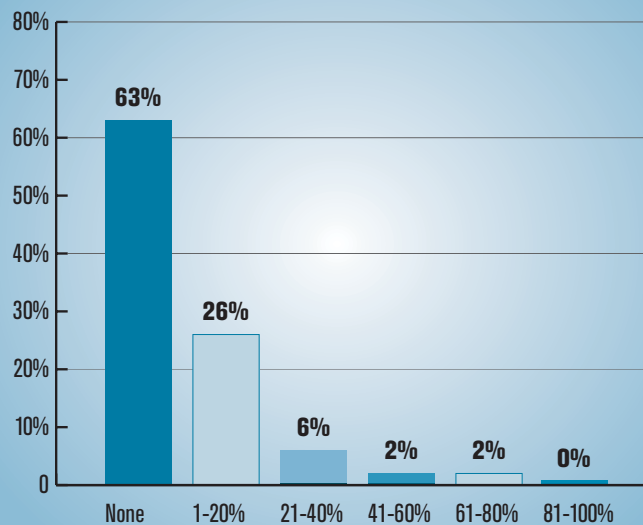## Figure 9. Percentage of Organizations Using ROI, NPV and IRR Metrics

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 599 Respondents

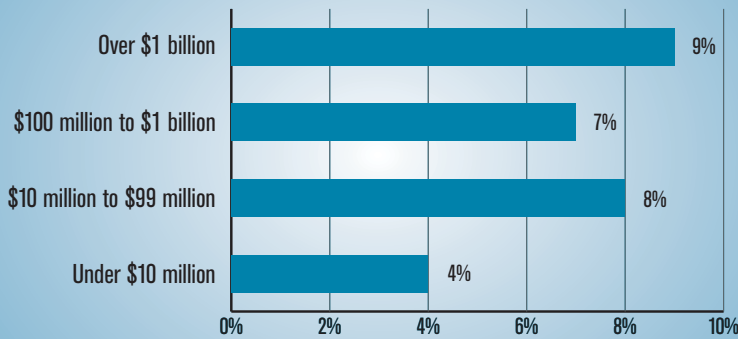## Figure 10. Percentage of Security Function Outsourced
(Numbers do not total 100% due to rounding.)

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 682 Respondents

Figure 11. Average Percent of Security Outsourced
By Organization Revenue

Over $1 billion	9%
$100 million to $1 billion	7%
$10 million to $99 million	8%
Under $10 million	4%

0% 2% 4% 6% 8% 10%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 682 Respondents

Figure 12. Organizations with External Insurance Against Cybersecurity Risks

80%
70%
60%
50%
40%
30%
20%
10%
0

Insurance: 25%
No insurance: 75%

CSI/FBI 2005 Computer Crime and Security Survey
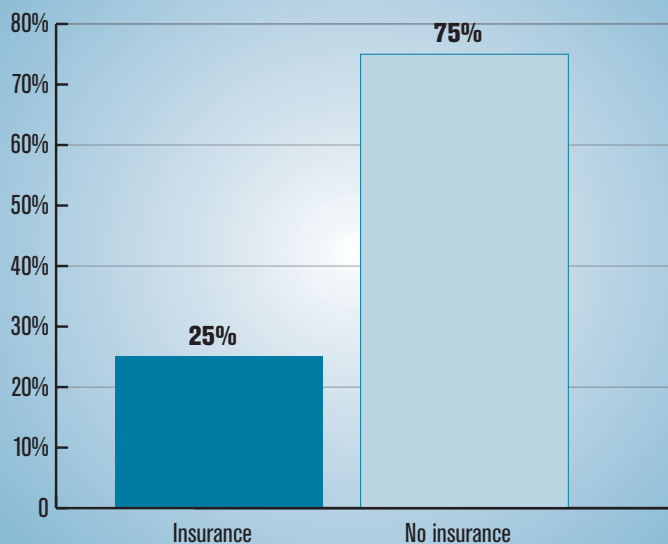Source: Computer Security Institute

2005: 652 Respondents

discussion of these metrics in security publications—particularly with a focus on more technical definitions of ROI analysis—may have led some respondents to realize that they weren't actually using the metrics they thought they were. The question, in other words, may have been answered more accurately based on a better understanding of the terms.

Two other areas of inquiry that were initiated in the 2004 CSI/FBI survey that were continued in the 2005 survey deal with outsourcing cybersecurity and the use of insurance as a tool for managing cybersecurity risks. Despite talk of increased outsourcing, the 2005 survey shows that outsourcing of computer security work has not increased over the past year. Less than 1 percent of respondents indicated that their organizations outsource more than 80 percent of the security function (see figure 10, page 9). As was the case last year, 63 percent of respondents indicated that their organizations do no outsourcing of the security function.

If one accepts the almost universally held view that there continues to be an increase in IT outsourcing, then the results over the past two years indicate that managers view the security function differently from other IT work. Figure 11
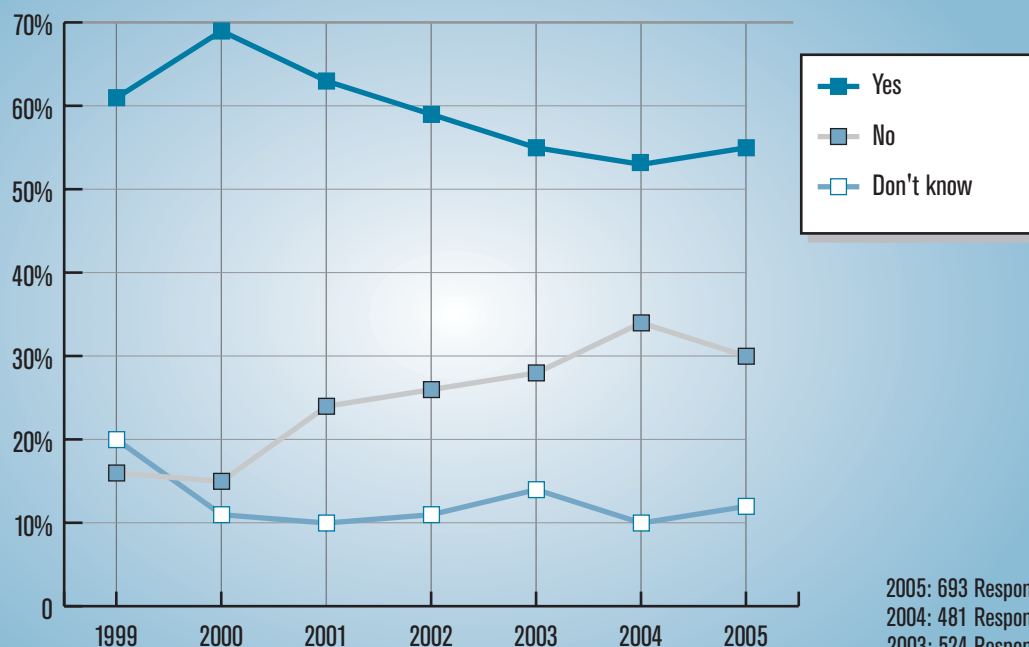
Figure 13. Unauthorized Use of Computer Systems within the Last 12 Months

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 693 Respondents
2004: 481 Respondents
2003: 524 Respondents
2002: 481 Respondents
2001: 532 Respondents
2000: 585 Respondents
1999: 512 Respondents

(page 10) shows the percentage of security outsourced by firm size. Although all the figures are low, the largest firms outsource the highest percentage of their security function.

Technical computer security measures such as use of passwords, biometrics, anti-virus software and intrusion detection systems cannot totally reduce an organization's risk of computer security breaches and the associated financial losses. Hence, it's natural that organizations would turn to insurance to deal with the risk of substantial financial losses that remains 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 12 (page 10), that only 25 percent of respondents indicated that their organizations use external insurance to help manage cybersecurity risks. The reported use of such insurance is roughly equal to last year's reported use. Thus, the 2005 survey indicates that cyber insurance is not yet gaining momentum, although many believe (including the authors of this study) that this situation will change over time.

3. For examples of such insurance firms and further analysis of cybersecurity insurance, 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.

Frequency, Nature and Cost of Cybersecurity Breaches

Turning to figure 13 (page 11), we can see that the decline in overall frequency of (successful) misuses of computer systems that began in 2001 may have come to a halt this year. The percentage of respondents answering that their organization experienced unauthorized use of computer systems in the last 12 months increased slightly from 53 percent last year to 56 percent this year. Furthermore, the percentage of respondents answering that there was no unauthorized use of their organization's computer systems decreased from 35 percent to 31 percent. The respondents not knowing if such an unauthorized use occurred increased from the low of 11 percent to 13 percent.

It's worth pointing out that this question queries a broader swath of undesired uses of computer and network resources than just those that might traditionally be called "attacks," particularly when comparing this question to the individual attack categories we discuss below. Both sharing offensive jokes among colleagues using a corporate e-mail server and storing downloaded music on an enterprise workstation in defiance of corporate policy would constitute unauthorized use, but wouldn't be reflected in traditional cybercrime categories.

The data presented in table 1 appear to indicate that the frequency of attacks is still decreasing. The percentage of respondents estimating that their firm experienced more than 10 computer security incidents reached the lowest level for all categories (total

Table 1: How Many Incidents? From the Outside? From the Inside?

How many incidents, by % of respondents	1–5	6–10	>10	Don't know
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
How many incidents from the outside, by % of respondents	**1-5**	**6-10**	**>10**	**Don't know**
2005	47	10	8	35
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, by % of respondents	**1–5**	**6–10**	**>10**	**Don't know**
2005	46	7	3	44
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

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
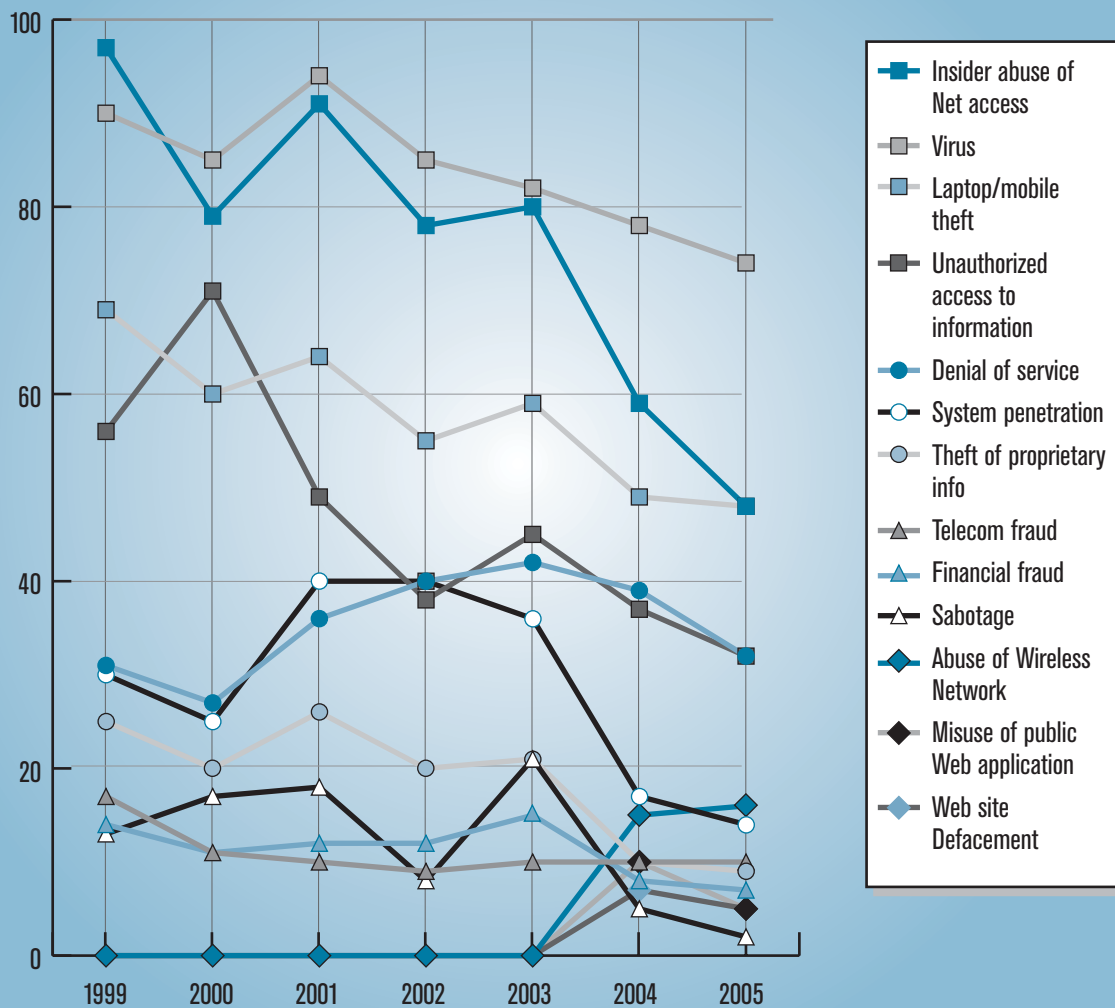2005: 453 Respondents

incidents, incidents originating from outside and incidents originating from inside), since 1998.[4] However, the small declines in the three "greater than 10 incidents" categories from last year to this year (from 12 percent to 9 percent in total incidents, from 9 percent to 8 percent in outside incidents and from 8 percent to 3 percent in inside incidents) may well be due to the increase in the "Don't know" response across all categories, so interpretation of these figures is problematic.

While it's difficult to interpret some aspects of table 1, the data do suggest that respondents detect events perpetrated by insiders about as often as by

4. The total incident percentage was lower in 1998 (9 percent) and lower still in 1997 (3 percent). It stood at a comparable 12 percent in 1996.
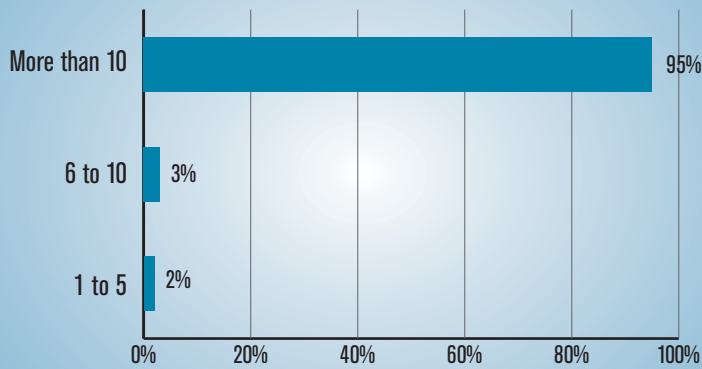

Figure 14. Types of Attacks or Misuse Detected in the Last 12 Months
By Percent of Respondents

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 700 Respondents

Figure 15. Percentage Experiencing Web Site Incidents

More than 10	95%
6 to 10	3%
1 to 5	2%

0%   20%   40%   60%   80%   100%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 258 Respondents

evidenced by figure 15, this year there was a total flip with 95 percent of responding organizations experiencing more than 10 Web site incidents and a mere 2 percent experiencing between 1 and 5 such incidents.

Respondents' estimates of the losses caused by type of computer security incident are shown in figure 16 (page 15). A number of important points may be inferred from figure 16, some of which are not readily accessible from inspection of the figure, but which are worthy of analysis.

outsiders, casting some doubt on the claims one often reads that the vast majority of crimes are commited by insiders.

Despite some variation from year to year, inside jobs occur about as often as outside jobs. The lesson here, though, surely is as simple as this: organizations have to anticipate attacks from all quarters.

Figure 14 (page 13) provides a visual demonstration that attacks of computer systems or (detected) misuse of these systems have been slowly, but fairly steadily decreasing over many years in nearly all categories. As seen in the figure, the only category showing a slight increase is the abuse of wireless networks. This category, along with Web site defacement, was only added last year.
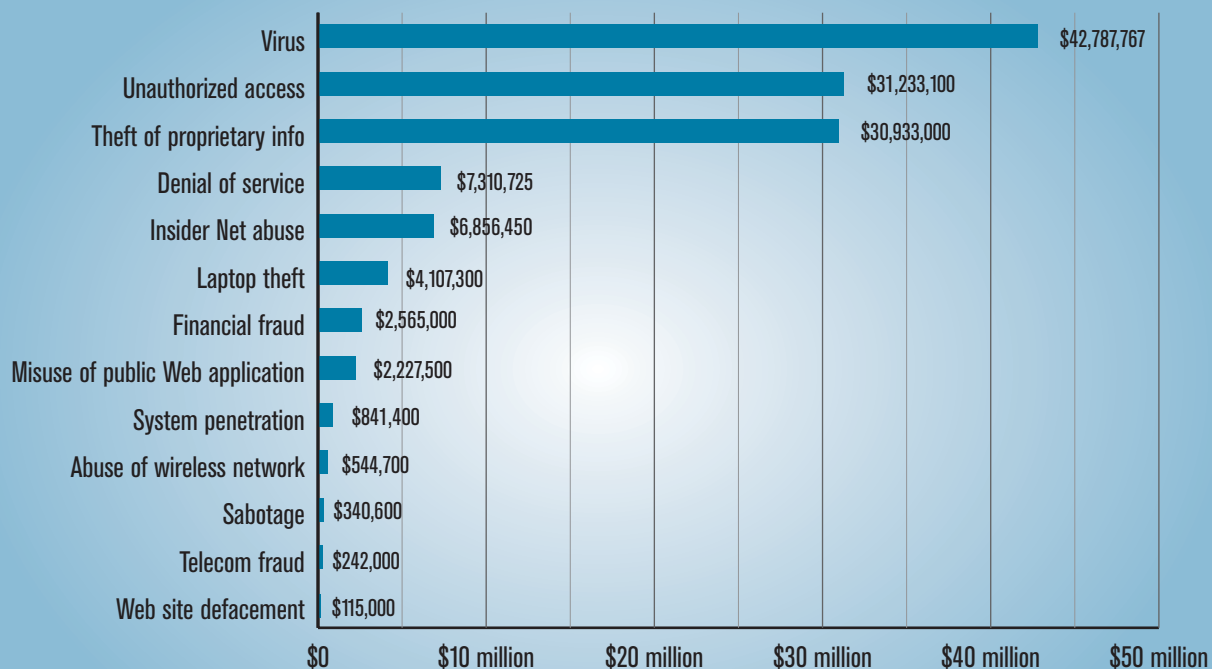
One of the most dramatic findings from this year's survey is the exponential increase in Web site incidents (figure 15). The 2004 survey found that 89 percent of those organizations responding experienced between 1 and 5 Web site incidents, but only 5 percent experienced more than 10 such incidents. As

First, the real story of losses is that the total losses reported (on a per respondent basis) declined dramatically. Total losses for 2005 were $130,104,542 for the 639 respondents that were willing and able to estimate losses—down from the $141,496,560 losses for the 269 respondents that were willing and able to estimate losses in 2004. Hence, losses per respondent declined from $526,010 to $203,606—a whopping 61 percent decline.

Beyond noting the overall decline in losses, figure 16 shows that the top three categories of losses—i.e., from viruses, unauthorized access and theft of proprietary information—swamped the losses from all other categories. The denial of service category is a distant fourth. Note also that the fastest-growing area of incidents, Web site defacement, is responsible for the least amount of losses. In fact, the low cost of these incidents would logically explain their total growth. That is, it would be reasonable to assume that since Web site defacement is not very costly to an organization, firms act in an

Figure 16. Dollar Amount Losses by Type

Type	Amount
Virus	$42,787,767
Unauthorized access	$31,233,100
Theft of proprietary info	$30,933,000
Denial of service	$7,310,725
Insider Net abuse	$6,856,450
Laptop theft	$4,107,300
Financial fraud	$2,565,000
Misuse of public Web application	$2,227,500
System penetration	$841,400
Abuse of wireless network	$544,700
Sabotage	$340,600
Telecom fraud	$242,000
Web site defacement	$115,000

Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
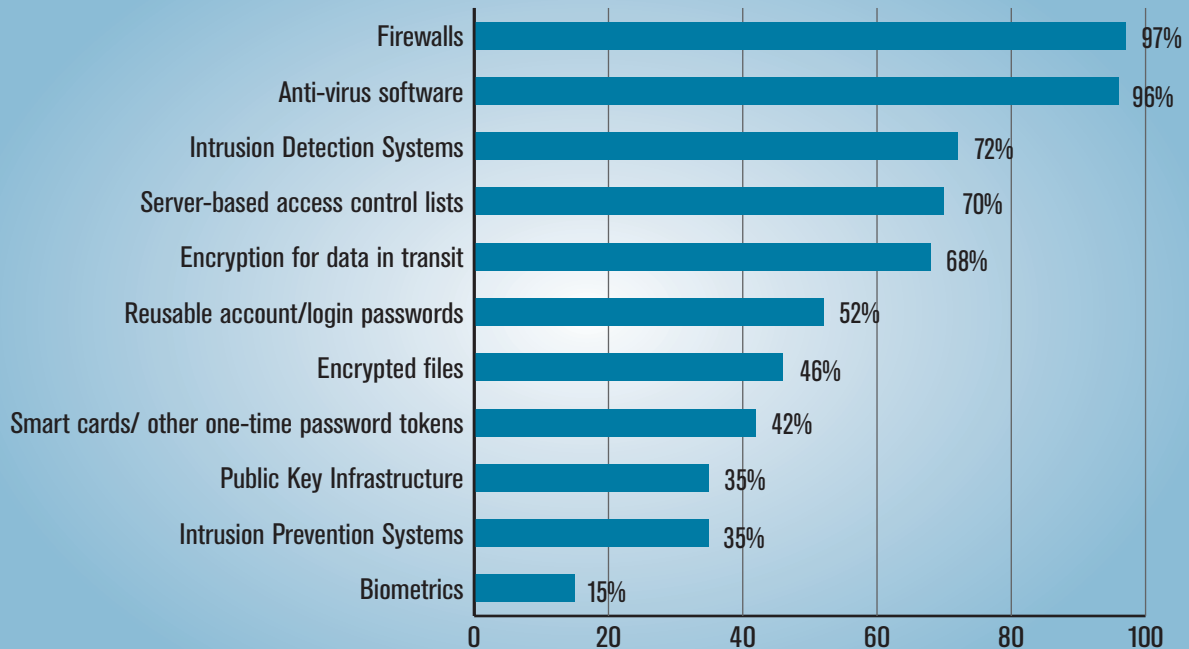Source: Computer Security Institute

2005: 639 Respondents

economically rational manner and do not spend much to prevent such attacks.

Although the general trend of losses is down, there were two areas of increase—unauthorized access to information (average loss per respondent up from $51,545 in 2004 to $303,234 in 2005) and theft of proprietary information (average loss per respondent up from $168,529 in 2004 to $355,552 in 2005). This can be explained by the increased awareness of, and improved technology to cope with some threat types, such as viruses. Security vendors and analysts love to discuss the possibilities for 15-minute saturation of the Internet (and the attendant gargantuan financial losses). We don't by any means dispute that very fast worldwide penetration is possible, but typical viruses detected in the past couple of years have spread far more slowly than their antidotes, at least where enterprise networks are concerned.

A final note on financial losses: the difficulty in interpreting overall downward trends is compounded by the difficulty of accurately measuring the implicit costs of losses associated with some crimes. We suspect respondents are more accurate than ever in accounting for their explicit costs (such as the cost of reinstalling software and reconfiguring computer systems). But we're equally suspicious that implicit losses (such as the lost future sales due to negative media coverage following a breach) are largely not represented in the loss numbers reported here. These implicit costs are difficult to measure, although they could be captured through the loss of market capitalization a publicly traded company may experience.

Figure 17. Security Technologies Used

Technology	Percentage
Firewalls	97%
Anti-virus software	96%
Intrusion Detection Systems	72%
Server-based access control lists	70%
Encryption for data in transit	68%
Reusable account/login passwords	52%
Encrypted files	46%
Smart cards/ other one-time password tokens	42%
Public Key Infrastructure	35%
Intrusion Prevention Systems	35%
Biometrics	15%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 687 Respondents

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 remained the same as those given last year (see figure 17) and the results are approximately the same.

Several categories addressed systems defending against network attack. Use of firewalls was reported by 97 percent of respondents and anti-virus software was reported as being used by 96 percent of the organizations. Intrusion detection systems were being used by 72 percent of the organizations and 70 percent used server-based access control lists. With the exceptions of the categories of smart cards and intrusion prevention systems, differences in reported use from last year were no greater than 5 percent. The use of smart cards and other one-time password tokens increased from 35 percent to 42 percent, while the in-trusion prevention system bandwagon reversed with a decline in use to 35 percent from 45 percent. 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.
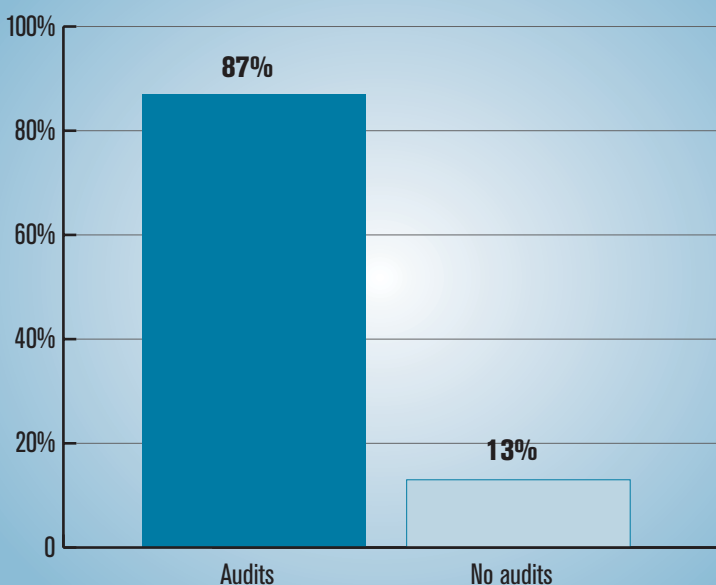
Security Audits and Security Awareness Training

Last year's CSI/FBI Computer Crime and Security Survey introduced several new questions that dealt with various aspects of improving computer security (beyond the use of technologies discussed above). The literature long has suggested using a security audit as

the first step toward a meaningful information security program. Thus, last year's CSI/FBI survey began the collection of data concerning the use of security audits. The 2004 survey found 82 percent of respondents indicating that their organization conducted security audits. As figure 18 shows, the percentage using information security audits increased this year to 87 percent. While the use of computer security audits is not universal, this year's survey provides preliminary evidence that the use of security audits is even more widespread today than as recently as one year ago.

Figure 18. Organizations Conducting Security Audits

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

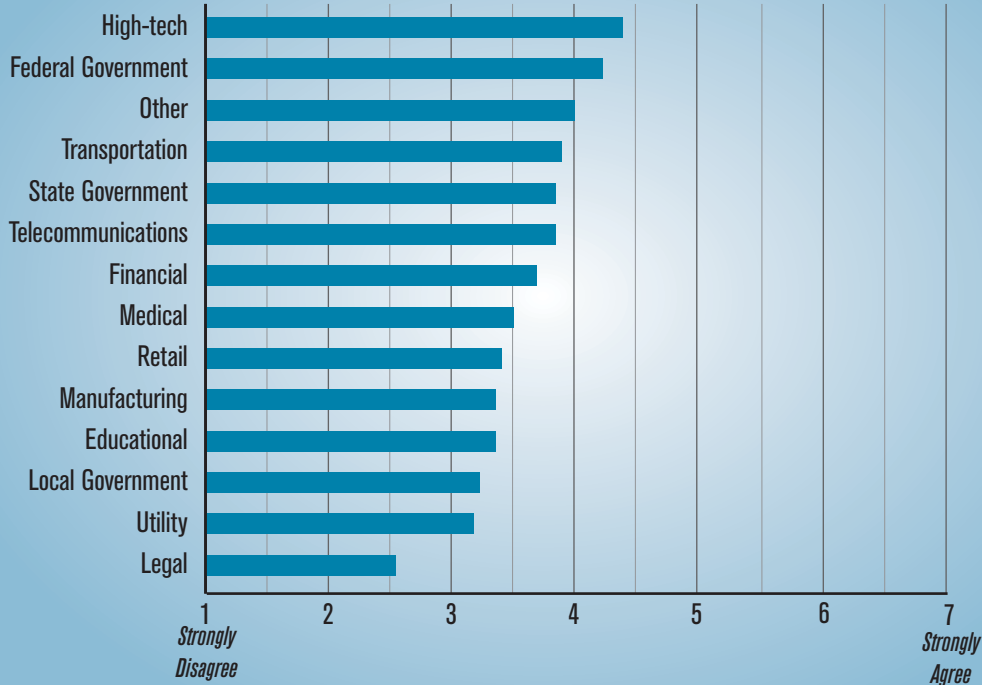2005: 681 Respondents

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 in this year's survey, originally introduced in the 2004 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 19 (page 18) illustrates that, on average, respondents from all sectors—except the high-tech sector and the federal government—do not believe that their organization invests enough in security awareness. These results are quite similar to those found in last year's survey, with the exception that the

high-tech sector appears to be getting more serious about spending on security awareness.

Survey participants were also asked to rate the importance of security awareness training to their organizations in each of several areas. Figure 20 (page 19) shows the percentage of respondents indicating that security awareness was very important (as measured by importance ratings of 5 or above on 7-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. Of the top five areas, *security policy* (70 percent), *security management* (70 percent), *access control systems* (64 percent) and *network security* (63 percent), were also the top four security areas identified by last year's respondents (although the percentages differed somewhat). The fifth security area that a majority of respondents identified as an area in which awareness training is important is *cryptography* (51 percent). Last year only 28 percent of

Figure 19. Organization Invests the Appropriate Amount on Security Awareness Training

Mean Values Reported on a Seven-Point Scale

High-tech, Federal Government, Other, Transportation, State Government, Telecommunications, Financial, Medical, Retail, Manufacturing, Educational, Local Government, Utility, Legal

1 Strongly Disagree — 7 Strongly Agree

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 698 Respondents

respondents identified this area as one in which security awareness training is important. Last year the fifth area identified was *economic aspects of computer security* (51 percent last year and 43 percent this year). The area in which security awareness was perceived to be the least valuable was security systems architecture.

Information Sharing

Although some of the largest and highest profile recent information security breaches (e.g., Citigroup, Bank of America and ChoicePoint) were not based on attacks of computer systems, the publicity surrounding these events has prompted additional calls for increased information sharing. Respondents to this year's survey indicated a disposition to share information about security intrusions—but no increase to share such information with either law enforcement or legal counsel.

Figure 21 (page 19) 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 73 percent of respondents indicated that their organization responds by patching security holes. Surprisingly, this is the lowest level in the seven-year period coved in figure 21. One explanation for this may be that the improved, automated approaches for patch dissemination and installation makes that process transparent to most.
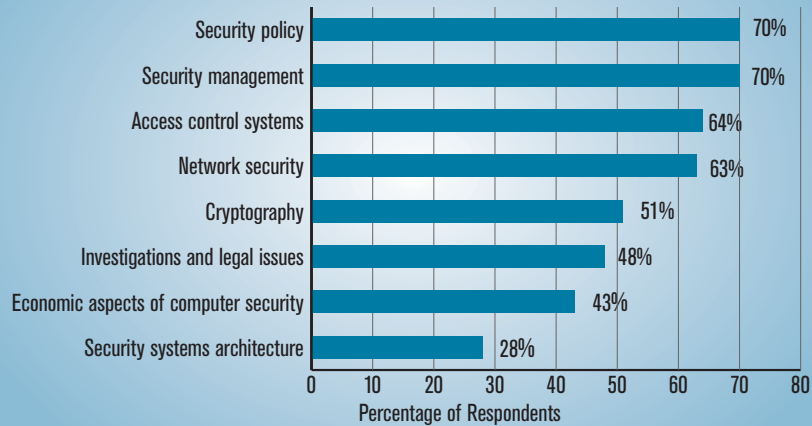
The next line down in the figure shows that 63 percent (100 percent–37 percent) of all respondents indicated that their organization shares information about a

security breach. The percentage of respondents who did not report their computer intrusions reached the lowest level for the seven-year period. Hence, the notion of information sharing may finally be taking hold. Surprisingly, as shown by the third and fourth line down respectively in figure 21, the percentage reporting to law enforcement (20 percent) remained at the multiperiod low reached last year, and the percentage reporting to legal counsel (12 percent) hit an all-time low.

Figure 22 (page 20) 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 7-point scale) in the decision not to report the computer intrusion. The predominant reason given for not reporting that was cited as being very important (by those indicating that their organizations would not report an intrusion to

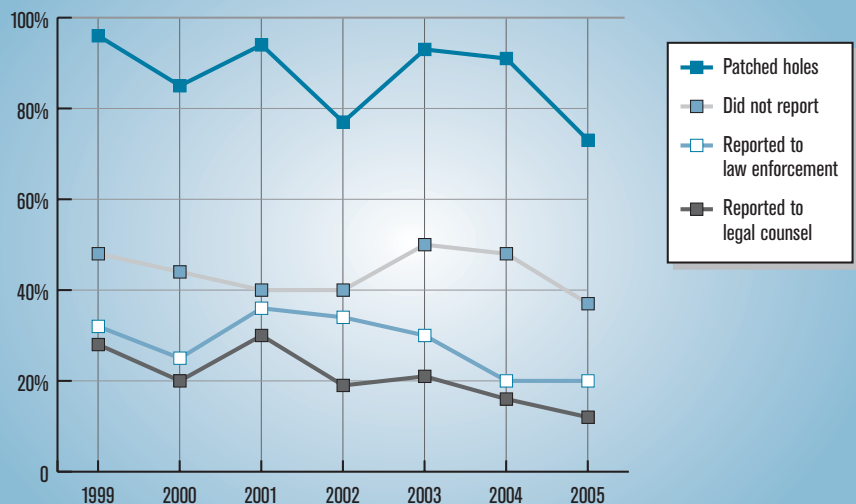**Figure 20. Importance of Security Awareness Training**

Percentage of Respondents Identifying as Important

Security policy	70%
Security management	70%
Access control systems	64%
Network security	63%
Cryptography	51%
Investigations and legal issues	48%
Economic aspects of computer security	43%
Security systems architecture	28%

Percentage of Respondents

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 694 Respondents

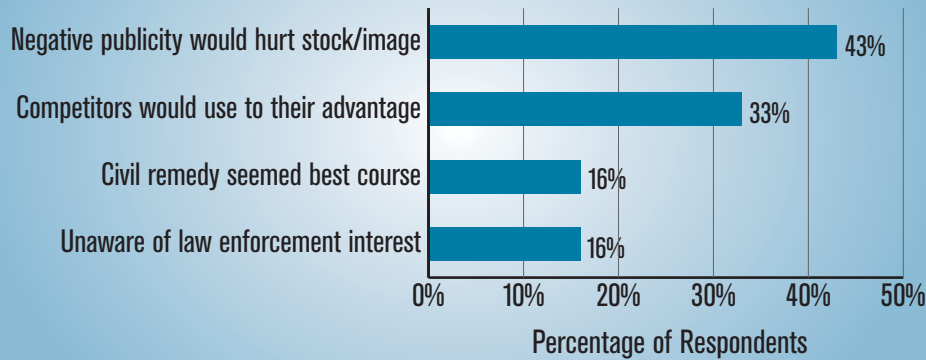**Figure 21. Actions Taken After Computer Intrusion(s) in the Last 12 Months**

- ■ Patched holes
- ■ Did not report
- □ Reported to law enforcement
- ■ Reported to legal counsel

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 320 Respondents

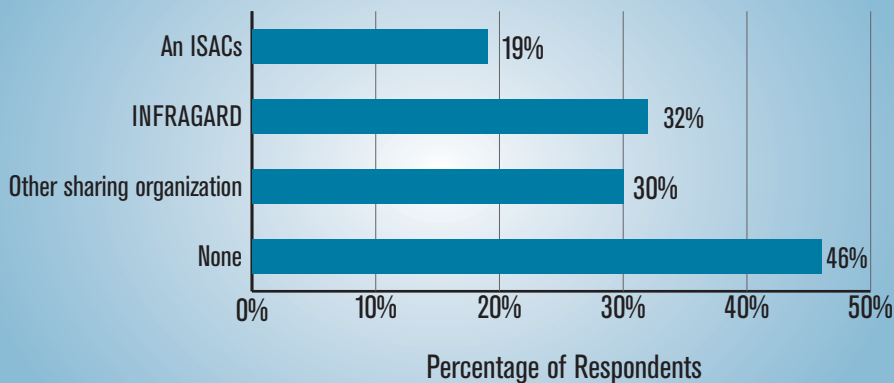## Figure 22. Reason Organization Did Not Report the Intrusion to Law Enforcement
Percentage of Respondents Identifying as Important

Negative publicity would hurt stock/image — 43%
Competitors would use to their advantage — 33%
Civil remedy seemed best course — 16%
Unaware of law enforcement interest — 16%

Percentage of Respondents

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 423 Respondents

Figure 23. Percentage of Respondents That Belong to an Information Sharing Organization

An ISACs — 19%
INFRAGARD — 32%
Other sharing organization — 30%
None — 46%

Percentage of Respondents

CSI/FBI 2005 Computer Crime and Security Survey
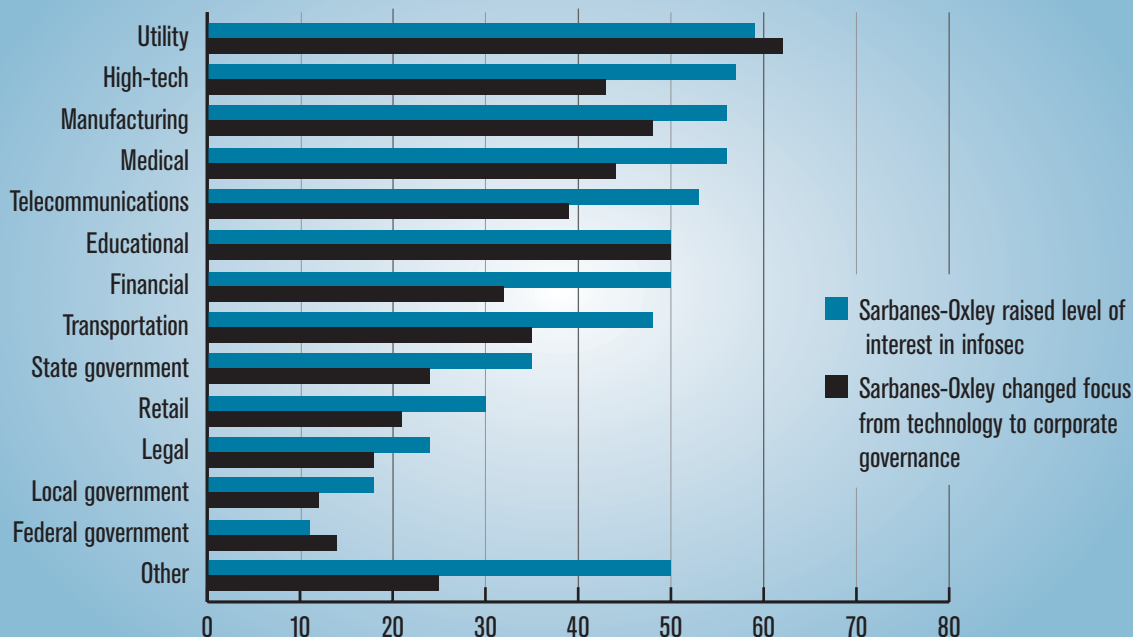Source: Computer Security Institute

2005: 667 Respondents

law enforcement) was the perception that resulting negative publicity would hurt their organization's stock and/or image.[5] While this reason is still the predominant reason given, the percentage of respondents identifying this reason as important dropped from 51 percent to 43 percent over the last year. As in last year's survey, 33 percent of respondents cited the advantage competitors could use as very important. Only 16 percent of respondents thought that using a civil remedy was a very important reason for not reporting the intrusion. The claim of being unaware of law enforcement's interest in the breach was also cited by 16 percent as a very important reason for failure

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 firm's stock price.

Figure 24. Impact of Sarbanes-Oxley Act on Information Security
Percentage of respondents that agree

Legend:
- Sarbanes-Oxley raised level of interest in infosec
- Sarbanes-Oxley changed focus from technology to corporate governance

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 679 Respondents

to report the intrusion. Thus, organizations seem to be aware, by and large, of law enforcement's role in combatting 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 the bottom bar in figure 23 (page 20) that about 46 percent of the respondents indicated that their organizations do not belong to any information sharing organization. About 32 percent of organizations in the survey belong to InfraGard, 19 percent belong to an ISAC and 30 percent to some other security sharing organization. These figures are roughly the same as those found in last year's survey (the first year this information was requested), although slightly more respondents this year (46 percent vs. 42 percent) indicated that their organizations belonged to no information sharing organization.

Overall, the survey results concerning the willingness of organizations to fully participate in information sharing of security breaches is consistent with recent theoretical work by three of the authors of this survey.[6]

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.

Effect of Sarbanes-Oxley Act

This year's survey asked a question first introduced in the 2004 CSI/FBI survey to determine the effect, if any, of the Sarbanes-Oxley Act on information security activities. As shown in figure 24 (page 21), the respondents in eight out of 14 sector categories (i.e., utility, high-tech, manufacturing, medical, telecommunications, educational, financial and other) believe the Sarbanes-Oxley Act is having an impact on their organizations' information security.[7]

In contrast, last year's survey showed an impact in only five of the 14 sector categories. Due to the phased-in nature of the Act, perhaps even a still greater impact of the Sarbanes-Oxley Act on information security will be seen in future years.

Concluding Comments

Computer-based information systems have been of critical importance to most major organizations for several decades. Since the mid-1990's, 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.[8]

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 much-needed knowledge base. As with earlier CSI/FBI Computer Crime and Security Surveys, the 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.

---

7. The new version of OMB Circular A-123—the implementing guidance for the Federal Managers Financial Integrity Act—requires federal 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.

8. 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 Gordon and Loeb (2005), forthcoming.*

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 24) who specialize in the economics of information security continued for a second year. These three have graciously joined me in coauthoring this report. I, along with 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 2005, both in a hardcopy, first-class mailing and in a Web e-mail blast. 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 re-search paper, for instance, you are granted permission here and do not need to contact CSI. For other uses, you must meet these requirements:

❏ 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 on page 24. 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 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, 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 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:
Shelagh Sayers, Special Agent
San Francisco FBI Computer Crime Squad
(415) 553-7400
Shelagh.Sayers@ic.fbi.gov, subject line: CSI Report
For general information: www.fbi.gov

For information on the CSI/FBI study:
Robert Richardson, Editorial Director
Computer Security Institute
(305) 455-8572
rrichardson@cmp.com
For general information: www.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 32 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:
32nd Annual Computer Security Conference & Exhibition
November 14–16, 2005
Marriott Wardman Park
Washington, D.C.
The world's largest conference devoted to computer and information security

NetSec 2006
June 12–14, 2006
The Phoenician Resort
Scottsdale, AZ
A balanced perspective of managerial and technical issues makes this the most popular conference devoted to network security.

33rd Annual Computer Security Conference & Exhibition
November 6–8, 2006
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 20, 2005
Chicago

September 21, 2005
Los Angeles

September 22, 2005
San Francisco

October 4, 2005
Dallas

October 5, 2005
Washington, D.C.

October 6, 2005
New York

FrontLine and TopLine Awareness Newsletters

Awareness Peer Groups

CSI Membership Benefits:
- Computer Security *Alert*
- Computer Security Journal (quarterly)
- CSI Member-only Archives
- Discounts on conferences, training and publications
- And much more

CSI
COMPUTER SECURITY INSTITUTE

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.