CSI Survey 2007

The 12th Annual Computer Crime and Security Survey

GoCSI.com

2007
CSI
COMPUTER CRIME AND SECURITY SURVEY

by Robert Richardson
Director, Computer Security Institute

For the past five years, this survey—perhaps the most widely quoted set of statistics in the industry—has shown a drop in average estimated losses due to cybercrime. This year, however, the tide has turned and respondents have reported a significant upswing.

Because this is the longest-running survey in the information security field, it's possible to see that losses climbed steadily before the loss numbers began to fall in 2002. The losses at their peak were still dramatically higher than they are this year. The drop from that peak came as a surprise to many and indeed no small amount of reflection has been invested in sorting out just how it could be that security practitioners thought they were losing less and less money.

There are, no doubt, many causes, but there were several surveys and studies not done by CSI where one could see drops both in the frequency and the cost of many different types of cybercrime. At least within the enterprise, most respondents to this survey over the years thought their better security performance was real enough (though, of course, a number of organizations continued to suffer catastrophic attacks and data breaches).

A drop in losses was welcome evidence that the efforts put into cyber security were showing some return on investment. At the same time, there was reason to believe that the downward trend couldn't continue indefinitely. A number of developments within the criminal world persuaded many knowledgeable observers that it was inevitable that the gains made would be given up with the arrival of newer, more insidious threats.

Though it's wrong to project a trend from a single year's results, and particularly from an informal survey such as this one, there is nevertheless a strong suggestion in this year's results that mounting threats are beginning to materialize as mounting losses.

This year's survey results are based on the responses of 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities.

This is the 12th year of the survey. In previous years, the survey was titled the CSI/FBI survey, but although our colleagues within the Bureau have continued to provide insight and opinion regarding the survey, the "FBI" nomenclature has been discontinued and the survey is now entirely administered by CSI.

We anticipate that this will give us more flexibility in the use and direction of our research efforts.

© 2007 by Computer Security Institute. All rights reserved.

KEY FINDINGS

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

- ❑ The average annual loss reported in this year's survey shot up to $350,424 from $168,000 the previous year. Not since the 2004 report have average losses been this high.
- ❑ Almost one-fifth (18 percent) of those respondents who suffered one or more kinds of security incident further said they'd suffered a "targeted attack," defined as a malware attack aimed exclusively at their organization or at organizations within a small subset of the general population.
- ❑ Financial fraud overtook virus attacks as the source of the greatest financial losses. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. If separate categories concerned with the loss of customer and proprietary data are lumped together, however, then that combined category would be the second-worst cause of financial loss. Another significant cause of loss was system penetration by outsiders.
- ❑ Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59 and 52 percent of respondents reporting each respectively.
- ❑ When asked generally whether they'd suffered a security incident, 46 percent of respondents said yes, down from 53 percent last year and 56 percent the year before.
- ❑ The percentage of organizations reporting computer intrusions to law enforcement continued upward after reversing a multi-year decline over the past two years, standing now at 29 percent as compared to 25 percent in last year's report.

In past survey reports, we've said relatively little about the challenges of gathering information about computer-related crimes. This is an informal survey, but then nearly all surveys in the field are conducted in a similar fashion. Looking across the broad scope of security reports, there would appear to be a great deal of variation in estimates of the prevalence of crimes and their impact. There is sometimes more concordance than might appear at first blush, however. Research reports have occasionally downplayed drops in attack frequency in favor of more compelling but less significant headlines.

The object here is not to quarrel with which conclusions should be drawn from other reports, and all reports including this one agree that the online world poses significant risks. In particular, the evidence is mounting that significant new threats are gathering force.

It goes almost without saying that vendors in the security space have a vested interest in playing up the notion that businesses face rapidly increasing risks, and one must approach their claims with appropriate skepticism.

Nonetheless, vendors aren't altogether in the wrong on this point. A large percentage of the security software industry is built on the practice of looking for the digital patterns (signatures) that identify known threats. Gartner estimates that worldwide security software revenue totaled $7.4 billion in 2005, a 14.8 percent increase from 2004 revenue of $6.4 billion; anti-virus software revenue made up $4 billion of that amount. In other words, virus pattern recognition

© 2007 by Computer Security Institute. All rights reserved.

accounted for 54.3 percent of the total security software industry. Further, anti-virus software is not the only security tool that looks for telltale signatures. Most of what firewall software and hardware does works along the same lines—but signature scanning is flawed.

Criminals have pushed the state of malware to a point where signature detection is less and less effective. Defenses built on these technologies are increasingly permeable. More is said about this later in the report, but even if the nature of attacks is changing, there are equally important questions to be asked about whether good or bad results reported by this survey's respondents are indicative of conditions across the broad scope of enterprises throughout the United States.

This author does not see the survey population in this study as representative of what might be conceived as a national pool of "people responsible for enterprise network security." There is almost certainly a skew created by the fact that this is the CSI community—members of the organization and those who move in its orbit (attending paid conferences and the like) without necessarily being members—and it's a community that is actively working to improve security. This pool, in short, doesn't stand in for the organizations in the United States that are simply not paying attention to security (and there are, unfortunately, all too many such organizations).

I do believe, though, that the survey samples the CSI community accurately, in large measure because it talks to such a large chunk of it. The issue of primary concern, in other words, isn't margin of error.

Rather, the issue that must be reckoned with is non-reporting error. Five thousand surveys are sent out and 494 were received back, meaning there was a 10 percent response rate. The question requiring judgment is that of whether those who chose to reply were markedly different than those who did not. Because the demographics of the respondents have remained very stable over the years, as has the basic makeup of the CSI community, it seems reasonable to assert that similar groups complete the survey year after year. Indeed, the vast majority of the questions yield virtually the same statistics year after year. The answers that have changed have been primarily the estimates of losses to cybercrime and we've seen them both rise and fall dramatically.

An additional element that must be factored in is simply that almost all financial information about crime losses are estimates. Some of them are probably altogether approximate guesses. At present, this is a circumstance that must simply be endured, because after all, there is to date no standard accounting for losses due to computer downtime.

In fact, the problem of figuring cyber losses can be quite complex. One often hears in conference presentations the bald statement that "if your company has a Web storefront and a denial-of-service attack takes you down, then you lose money for every minute you're down." It seems obvious, but then again there's no particular reason to believe it's true.

If a customer has decided to buy a book from a prominent online bookseller, it may be quite reasonable to assume that the customer who can't complete the transaction when they get home from the office will complete the same transaction after dinner that evening. Of course no business wants to shut out customers, but the actual cost of downtime—probably the firmest metric among many relatively approximate measures of cybercrime losses—isn't as obvious as we might hope.

All that said, the rough reckoning of seasoned professionals is nevertheless generally on-target and worth study. When a group of professionals reports a significant reversal in a five-year trend of diminishing losses, we should be inclined to perk up our ears.

© 2007 by Computer Security Institute. All rights reserved.

DETAILED SURVEY RESULTS

NOTE: Dates on the figures refer to the year of the report (i.e., 2007). The supporting data is based on the 2006 calendar year.

About the Respondents

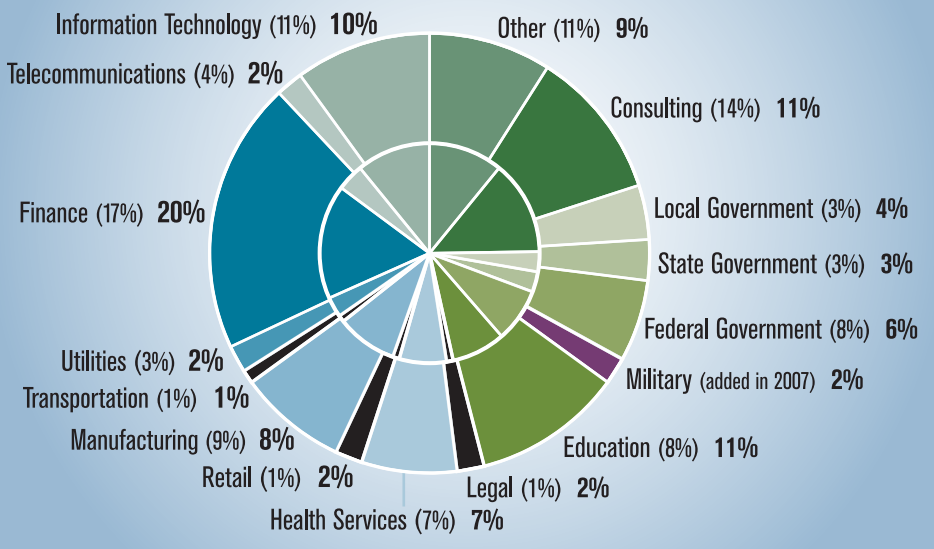
The CSI survey has always been conducted anonymously as a way of enabling respondents to speak freely about potentially serious and costly events that have occurred within their networks over the past year. As previously mentioned, this introduces a difficulty in interpreting the data year over year, because of the possibility that entirely different people are responding to the questions each time they are posed. We nevertheless think it is a reasonable judgment to say that the pool remains uniform in its makeup. In part, that's because the survey is sent to roughly the same group: the CSI community. That includes both paid members of the organization and paid attendees of CSI conference events.

As **figure 1** shows, organizations covered by the survey include many areas from both the private and public sectors. The outer ring shows the current year's statistical breakdown, while the inner ring shows the prior year's values, fairly similar though not as much as in prior years in part because new categories (military and law enforcement) were added as possible answers this year. Note, however, that responses from the financial sector did grow modestly this year.

The sectors with the largest number of responses came from the financial sector (20 percent), followed by consulting (11 percent), education (11 percent), information technology (10 percent), and manufacturing (8 percent). The portion coming from government agencies (combining federal, state and local levels) was 17 percent and educational institutions accounted for 8 percent of the responses. The diversity of organizations responding was also reflected in the 9 percent designated as "Other."

Figure 1. Respondents by Industry Sector

(Numbers do not total 100% due to rounding.)
(No respondents identified themselves as law enforcement.)
(2007 = outer circle, percentages in bold)
(2006 = inner circle, percentages in parentheses)



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 494 Respondents

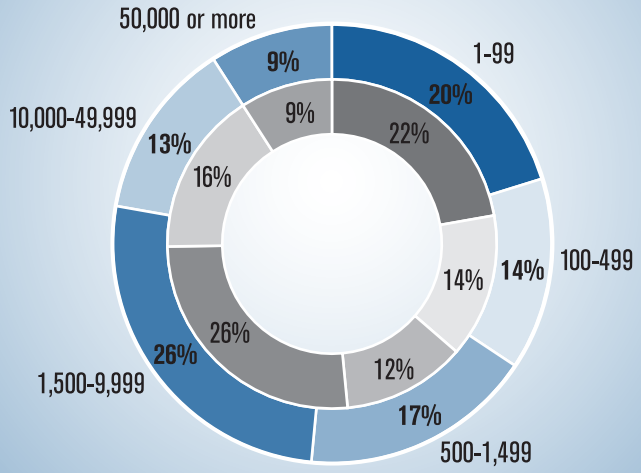
© 2007 by Computer Security Institute. All rights reserved.

Figure 2 shows that the survey pool leans toward respondents from large enterprises. Organizations with 1,500 or more employees accounted for a little less than half of the responses. As the chart shows, the percentages of respondents from the various categories remained very close to this question's breakdown in 2006. And that breakdown clearly favors larger organizations, at least compared to the U.S. economy as a whole, where there is a preponderance of small businesses.

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 36 percent generating annual revenues in excess of $1 billion. Nevertheless, 24 percent of the responding firms generated annual revenues under $10 million. Comparing these numbers with our earlier surveys (not shown here), roughly the same sized firms responded over

Figure 2. Respondents by Number of Employees

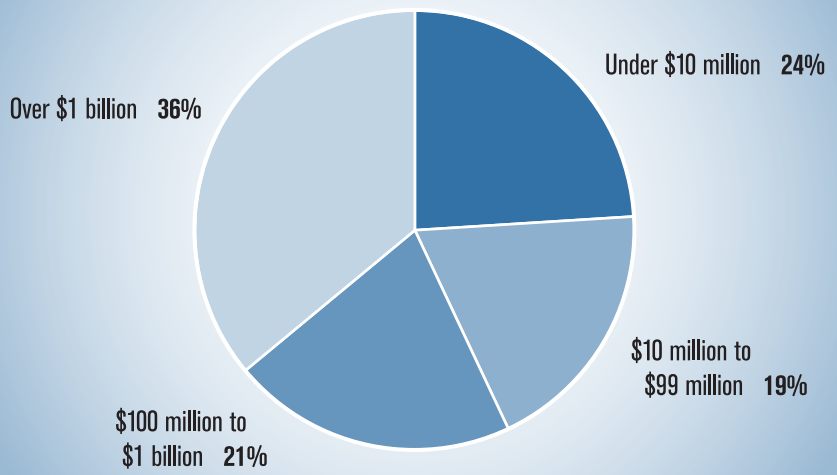
(Numbers do not total 100% due to rounding.)
Inner circle=2006; outer circle=2007



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 485 Respondents

Figure 3. Respondents by Organization Revenue



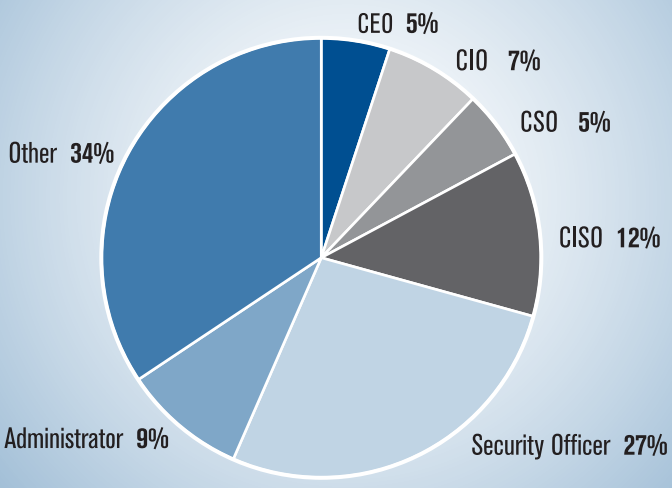
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 373 Respondents

© 2007 by Computer Security Institute. All rights reserved.

Figure 4. Respondents by Job Description

(Numbers do not total 100% due to rounding.)
(Less than 1 percent of respondents identified themselves as Chief Privacy Officers.)



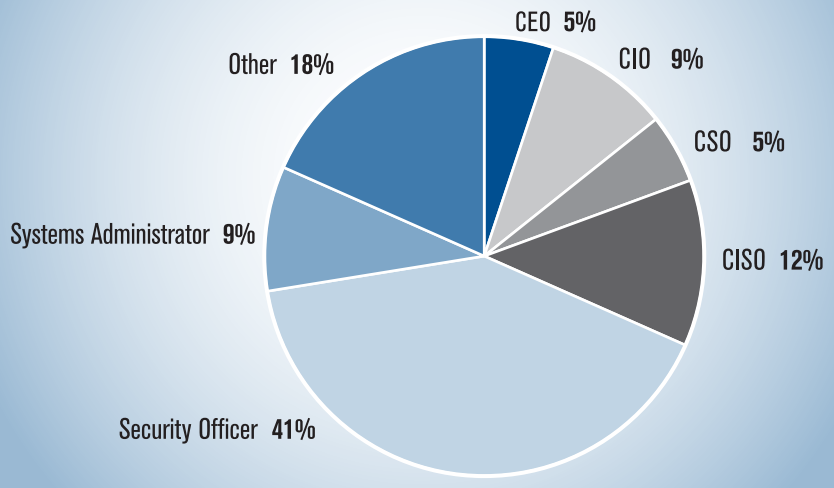
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 494 Respondents

Figure 5. Respondents by Job Description

With Some 'Other' Responses Recategorized Where Appropriate

(Numbers do not total 100% due to rounding.)
(Less than one percent of respondents identified themselves as Chief Privacy Officers.)



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 494 Respondents

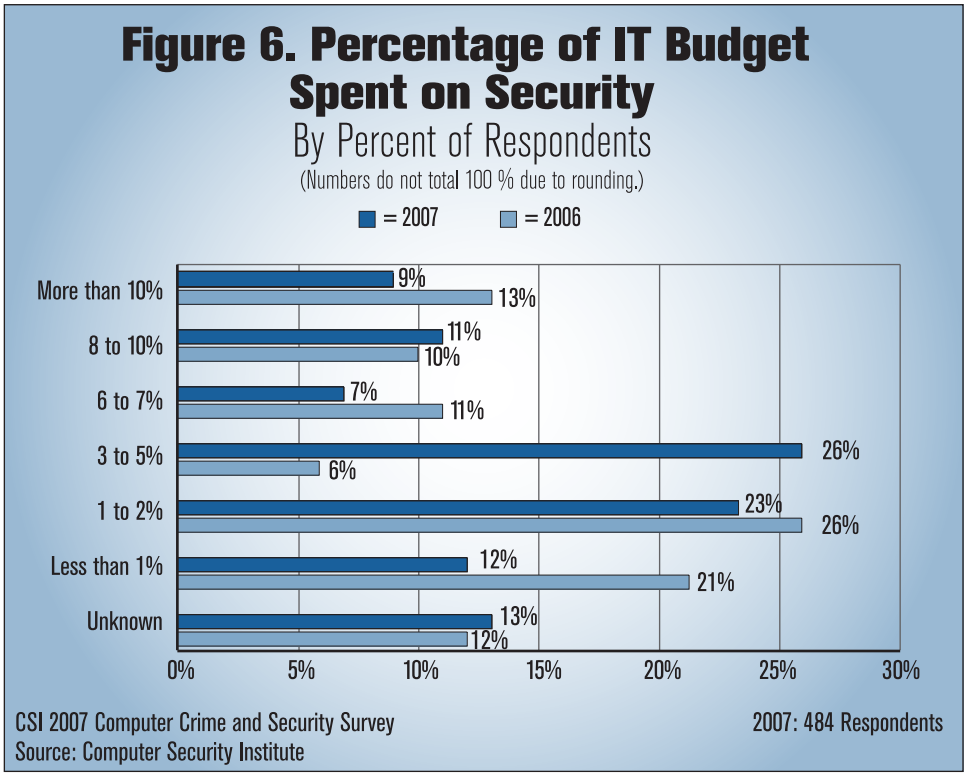
time—again allowing us to make some meaningful trend analyses.

For the fourth consecutive year, respondents were grouped by job title. **Figure** 4 illustrates that 29 percent of respondents were senior executives with the titles chief executive officer (CEO) (5 percent), chief information officer (CIO) (7 percent), chief security officer (CSO) (5 percent) or chief information security officer (CISO) (12 percent). The single largest category of respondents (27 percent) had the job title of security officer (up 4 percent from last year). An additional 9 percent of respondents had the title of system administrator, while 34 percent had various other titles. Last year's questionnaire turned up two respondents who ticked the checkbox for chief privacy officer, but this year only one turned up, leading us to suspect that the title as such doesn't have traction in the enterprise world.

A closer look at the fill-in answers provided along with the selection of "Other" affords an opportunity to note other titles that have prominence in the field at present. In

© 2007 by Computer Security Institute. All rights reserved.

particular, "Director of Security" and other similar variants, along with variations of titles having both "manager" and "security" in the title. If one conservatively remaps all "director" and "manager" replies to the "Security Manager" category and likewise remaps chief technology officer and similar C-suite variants into the "CEO" category, the "Other" category is reduced to 18 percent and the resultant chart is shown in **figure 5** (page 6).



Remapped or not, it is clear that the preponderance of respondents have full-time security responsibilities within their organizations. Additionally, as we've noted in this survey before, it's quite likely that the survey pool 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

This survey has always contained a number of questions about the costs of computer crime, but for the past four years, it has also explored the budgeting and financial management of information security risk. In this year's survey, 61 percent said that their organizations allocated 5 percent or less of their overall IT budget to information security (**figure 6**). This is comparable to last year's results, but a bit higher as 53 percent indicated they fell into this range last year. A quick comparison of the bars at the 3 to 5 percent level shows a significant uptick this year, and it's worth noting in tandem with this that last year 47 percent said their organization allocated less than 3 percent of the total IT budget, whereas this year only 35 percent fell into that range.

The general picture is that security program budgets are slightly up. Of course, expressing the budget as a percentage of the IT budget means that the actual number of dollars spent depends on whether the IT budget is growing or shrinking. It's growing, but at a slower rate than in previous years and, one suspects, without radically changing the security funding scenario at most organizations. Projections for 2008 from major analyst firms tend to center on growth in overall global IT spending within 1.5 percent of a 5 percent growth over the previous year. (IDC says 6.3, Merrill Lynch says 4.2, Forrester Research says 5 (down from 8)).

We should note that the question asked in this year's survey clarified that the answer should be expressed as a percentage of the IT budget, even if not all the money

© 2007 by Computer Security Institute. All rights reserved.

in the security budget came from IT. Increasingly security is viewed as a problem that is far broader than technology alone—in some instances part of the security budget comes from audit and legal departments. Some years back there were some prominent leaders of the industry who felt that security solutions would, in the final analysis, be almost exclusively technical solutions, but one would be hard-pressed to find that point of view espoused today. There have been too many data breaches driven by simple human error and carelessness.

Training individuals with responsibility for sensitive enterprise databases is clearly part of the security agenda, and toward that end a new question was added in this year's survey, asking what percentage of the security budget was allocated for awareness training. Almost half—48 percent—spend less than 1 percent of their security dollars on awareness programs (**figure** 7). While this may be the case simply because some forms of awareness training (such as putting reminders on corporate intranet sites) aren't expensive, one is tempted to conclude that while the industry talks a good game about teaching users how to be good stewards of company network resources, they don't yet put real dollars behind the proposition.

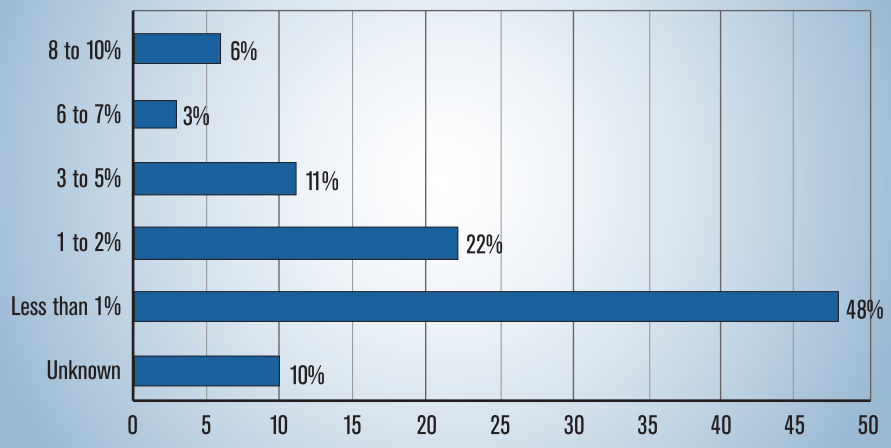
As far as the author is aware, this is the only currently available statistical information on what expenditures are made for security awareness training.

Business Justifications

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 CFO), 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 financial metrics for quantifying the cost and benefits of computer security expenditures (**figure 8**, page 9). 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.

In last year's survey, 42 percent of respondents indicated their organizations used ROI as a metric, 19 percent used NPV, and 21 percent used IRR. This year, 39 percent said they use ROI, 21 percent use

Figure 7: Percentage of IT Security Budget Spent on Awareness Training
By Percent of Respondents



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 475 Respondents

© 2007 by Computer Security Institute. All rights reserved.

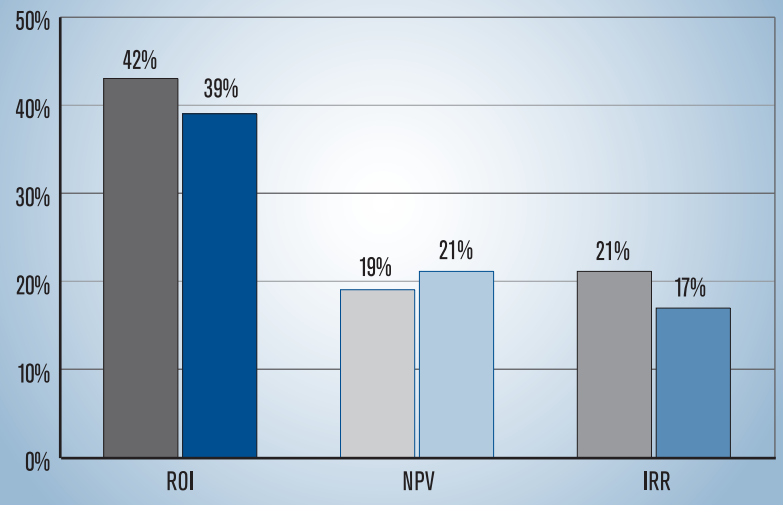
NPV and 17 percent use IRR. This tracks closely with the numbers from two years ago, when the tallies were 38 percent, 18 percent, and 19 percent, respectively. In short, there's reason to believe that things are about where they were when we started asking this question. To put it another way, there's no sudden groundswell in the use of NPV, nor a retreat from approaches that consider the time value of money back to "simpler" ROI calculations.

As a side note, all these numbers remain lower than they were in 2004, the first year the question was included in the survey. At that time, the results were 55 percent, 25 percent, and 28 percent, respectively. As you'd perhaps expect, ROI is still by far the most popular metric used. This may be in part because "return on investment" is a phrase that gets a lot of use as a loose way of referring to the time required to recoup an investment—not, strictly speaking, an accurate interpretation of the term as used in the capital accounting profession.

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 2007 survey shows that outsourcing of computer

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

(2007 figures in blue. 2006 figures in gray.)

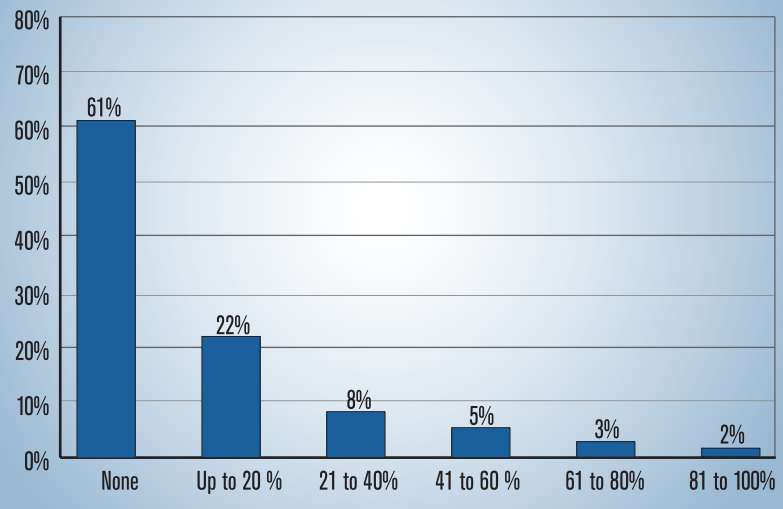


CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 314 Respondents

Figure 9. Percentage of Computer Security Functions Outsourced

By Percent of Respondents

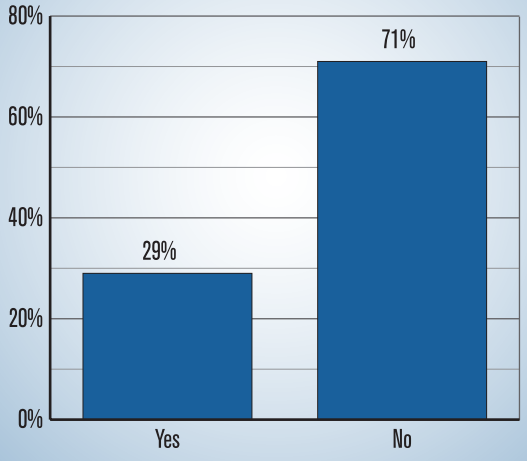


CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 479 Respondents

© 2007 by Computer Security Institute. All rights reserved.

Figure 10. Does Your Firm Have Any External Insurance Policies to Manage Its Cybersecurity Risks?

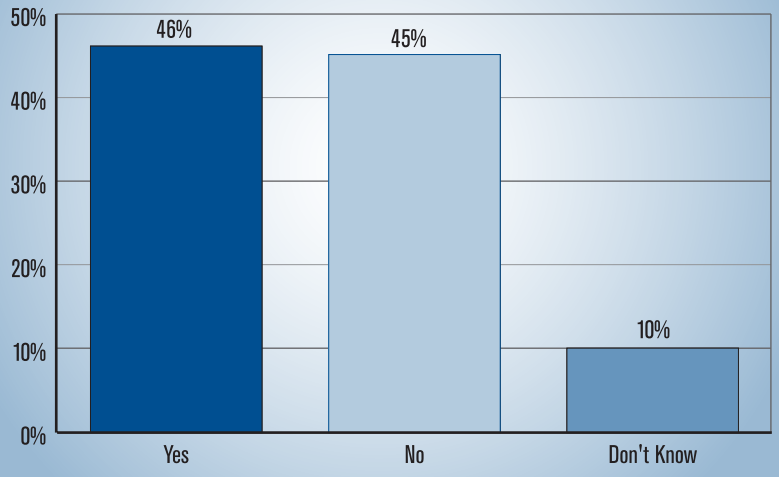


CSI/FBI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 454 Respondents

Figure 11. Did Your Organization Experience a Security Incident in the Past 12 Months?

By Percent of Respondents
(Numbers do not add up to 100% due to rounding.)



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 487 Respondents

security work remains at approximately the same levels found in the previous three surveys. Some two percent of respondents indicated that their organizations outsource more than 80 percent of the security function (**figure 9**, page 9). This year, 61 percent of respondents indicated that their organizations do no outsourcing of the security function—precisely the same percentage as last year. While there's certainly a market for outsourcing some kinds of security tasks (security testing of customer-facing Web applications being one such example) where the specialized nature of the work and the ability to segregate the task from access to key enterprise assets make outsourcing more appealing, it doesn't appear that appetite for such outsourcing is growing overall.

Cyber insurance (**figure 10**) is another area where we haven't seen noticeable growth, even though cyber insurance is the sort of concept that would seem, on the face of it, likely to catch hold. Purchasing cyber insurance allows organizations to reduce risks that remain, even when these organizations are using technical computer security measures such as one-time passwords, biometrics, anti-virus software and the like. A number of companies do offer such policies, but because of the lack of good actuarial data

© 2007 by Computer Security Institute. All rights reserved.

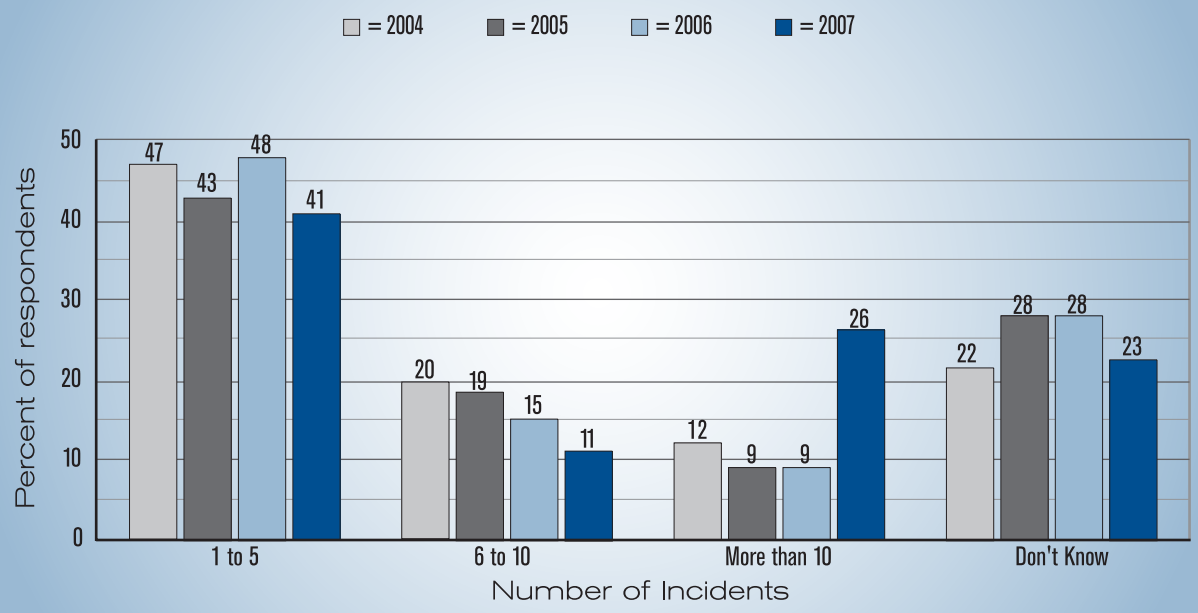
on which to base insurance rates, providers have the incentive to add additional risk premiums to the prices they charge for these policies.[1] Over time one would expect that as insurance companies gain experience with this new product, the additional risk premiums would shrink and prices for such policies would become more attractive. This, together with organizations becoming more familiar with this new insurance product, would lead one to expect that the use of cyber insurance should be growing each year. We haven't seen that, however. This year, as last year, 29 percent of respondents indicated that their organizations use cyber insurance. This number is up from the 25 percent found in the 2005 Survey, but that in turn is down from the 28 percent of respondents reported using cyber insurance in the 2004 survey, the first year this question was asked. While the authors speculated last year that use of cyber insurance might be on the rise, this year's flat response perhaps indicates otherwise. It's of course impossible at this point to say whether this form of risk transfer has reached its full potential or whether its adoption is going to be slower than might have been anticipated.

Frequency, Nature and Cost of Cybersecurity Breaches

Even though average losses are up markedly this year, computer security incidents apparently occur with less frequency within organizations (**figure 11**, page 10).

1. *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.*

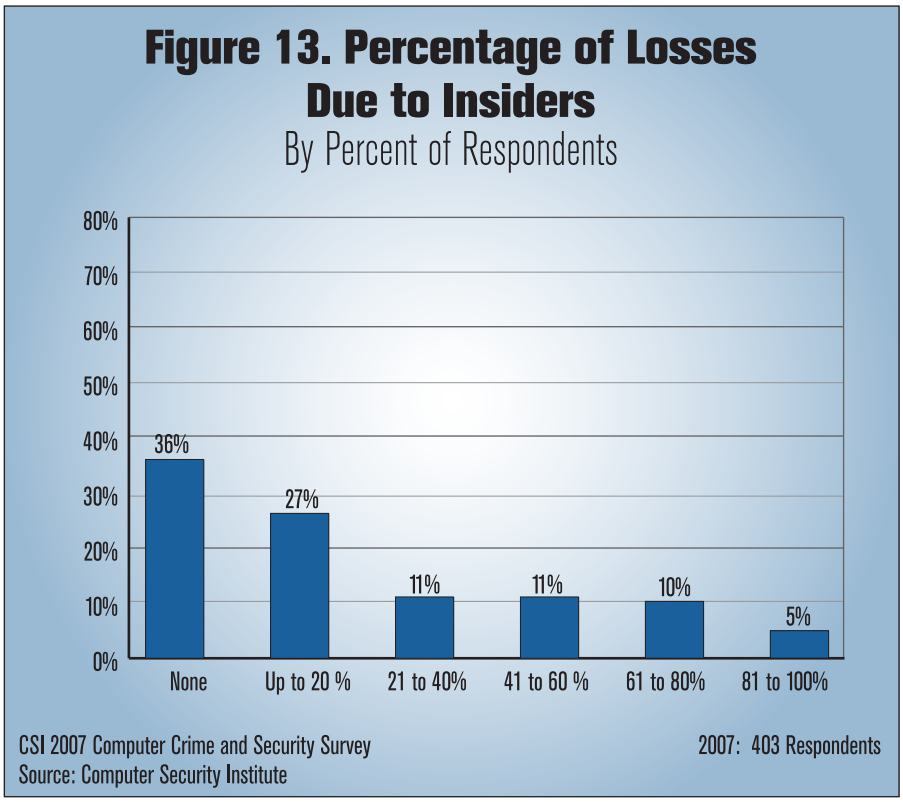
Figure 12. How Many Incidents in the Past 12 Months?



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 280 Respondents

© 2007 by Computer Security Institute. All rights reserved.



When respondents were asked rather straightforwardly whether anything amiss had occurred—other than quick network scans that may or may not signal an attack—only 46 percent said that they have. This figure is down from 52 percent last year and 56 percent the year before. Overall, this is down from a peak of 70 percent in 2000.

A follow-up question on the survey asks about the number of incidents that occurred at organizations where incidents were detected. The response, shown in **figure 12** (page 11) indicates that respondents who detected incidents tended to detect more of them than in past years, with the number who detected more than 10 incidents jumping from 9 to 26 percent.

Last 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** shows the percentage of losses that respondents attributed to insiders. As can be seen in the figure, slightly more than one-third (36 percent) of respondents believe that insider threats account for none of their organization's cyber losses—this is up from 32 percent last year. Another 27 percent of respondents attribute a percentage of losses greater than zero but less than 20 percent to actions of insiders. Hence, the remaining 37 percent of respondents attribute a percentage of their organization's losses greater than 20 percent to insiders. In fact, 5 percent of respondents thought that insiders account for more than 80 percent of their organization's losses (it was 7 percent last year). While some respondents believe that significant amounts of their losses are due to insiders, well over half think that only a small amount of financial losses are due to insiders.

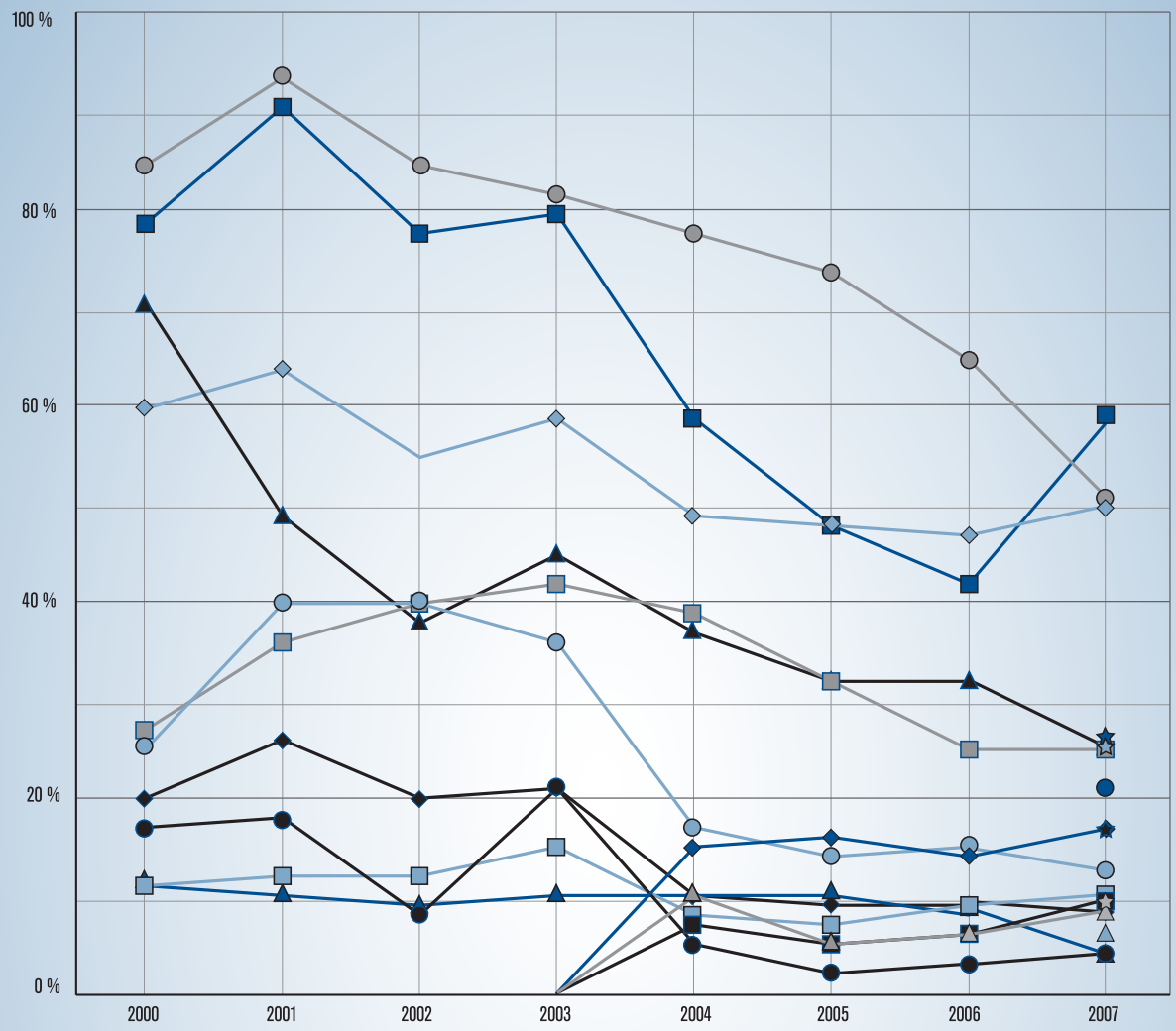
A great deal is made of the insider threat, particularly by vendors selling solutions to stop insider security infractions. It's certainly true that some insiders are particularly well-placed to do enormous damage to an organization, but this survey's respondents seem to indicate that talk of the prevalence of insider criminals may be overblown. On the other hand, we're speaking here of financial losses to the organization, and in many cases significant insider crimes, such as leaking customer data, may not be detected by the victimized organization and no direct costs may be associated with the theft.

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. For this year, however, respondents indicated a jump in insider abuse of network resources from 42 to 59 percent. Additionally, there was a slight increase, from 47 to 50 percent, in laptop and mobile device theft.

© 2007 by Computer Security Institute. All rights reserved.

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

By Percent of Respondents



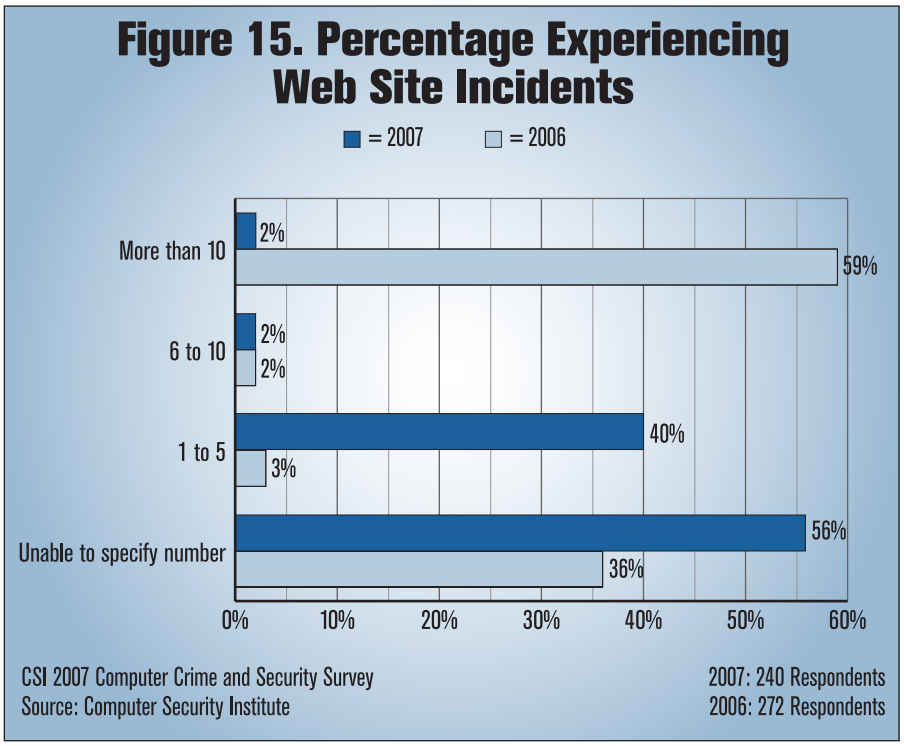
TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization**	21%
Theft of customer / employee data**	17%
Abuse of wireless network*	17%
System penetration	13%

TYPE OF ATTACK	2007
Financial fraud	12%
Password sniffing**	10%
Web site defacement*	10%
Misuse of public Web application*	9%
Theft of proprietary information (intellectual property)	8%
Exploit of the organization's DNS server**	6%
Telecom fraud	5%
Sabotage	4%

***Added in 2004 survey**
****Added in 2007 survey**

CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 436 Respondents



Several less-prevalent categories—financial fraud, system penetration, sabotage, Web site defacement and misuse of public Web applications—all showed small upticks as well.

The survey asks a question specifically about public Web site incidents and this year's responses were markedly different than last year's in terms of how many incidents a victim organization typically suffered. In 2006, the number reporting more than 10 incidents was 59 percent, whereas this year only 2 percent said they had that many incidents (**figure 15**). Conversely, the 2006 survey showed only 3 percent having 1 to five incidents, whereas this year, 40 percent of respondents fell into that category.

Respondents' estimates of the losses caused by various types of computer security incident dropped significantly for five consecutive years, including last year. But not so this year, when the total losses reported were up substantially even though the number of respondents answer the question fell. In total, 194 responses yielded losses of $66,930,950 (see **figure 16**), up from $52,494,290 (for 313 respondents) in 2006.

The most useful way to look at these losses, of course, is in terms of average losses per respondent, and this is shown in **figure 17** (page 16). This year, the average loss per respondent was $345,005 up from $167,713 last year.

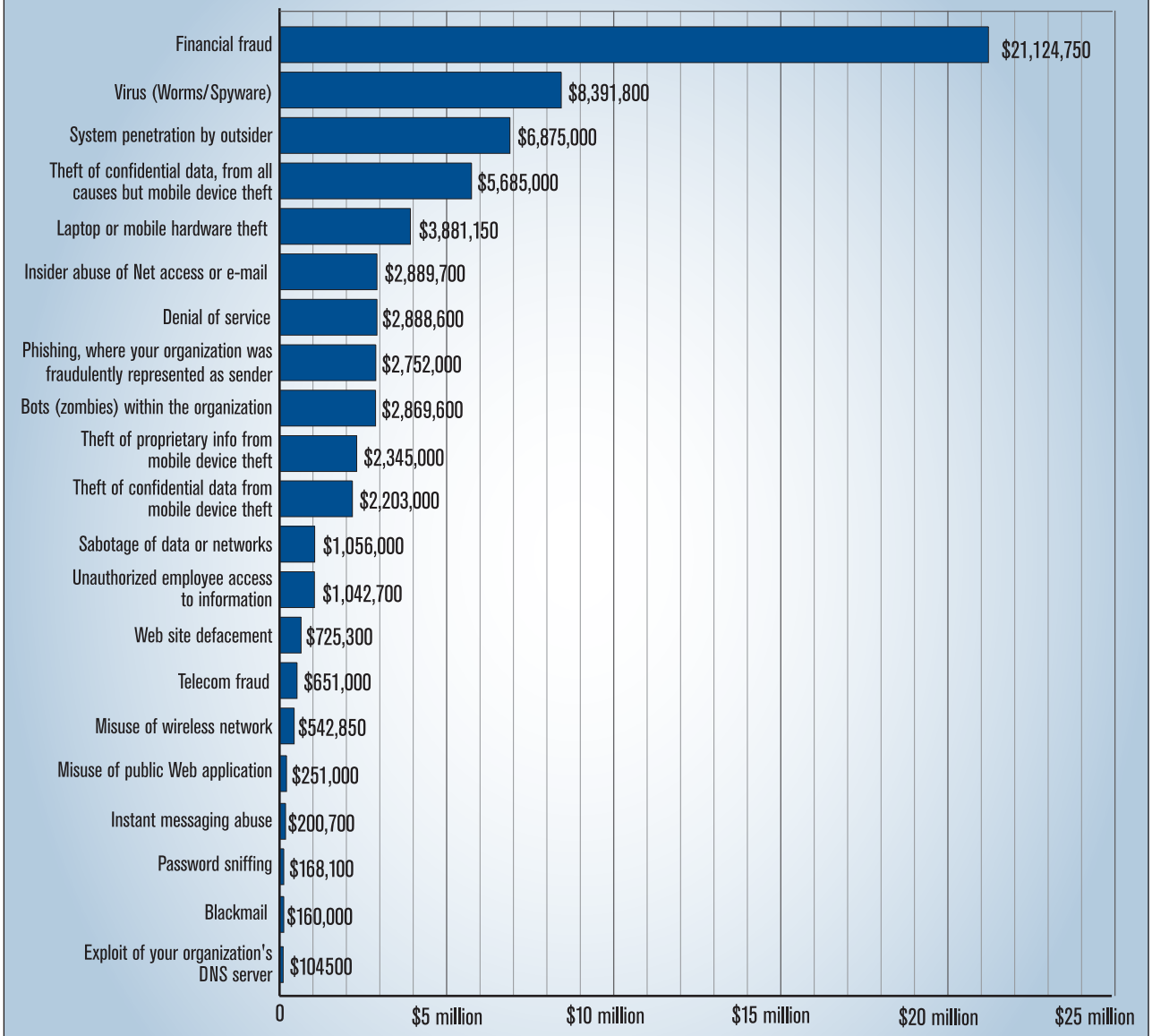
This year, even fewer respondents were willing to share details of their financial losses—194 respondents answered questions about dollar losses. It is quite possibly significant that the number of respondents has dropped. For many years, some critics of the survey have suggested that survey takers simply weren't sharing their losses and therefore losses were declining. This theory had a potential shortcoming, however, namely that the percentage of respondents sharing dollar losses had remained very nearly one-half of the overall pool for several years running. Roughly the same number of people in the same size overall pool with consistent demographic breakdowns year over year were saying that they thought they'd lost less and less money.

There were reasonable explanations for why lower loss numbers might be reported. Perhaps the likeliest candidates can be oversimplified to say that basic security measures like anti-virus software work. Surely it cannot be unreasonable to imagine some success has come from all our security efforts.

We should keep in mind that losses reported in this survey were suffered by enterprises, not individual consumers. The biggest losses reported by organizations throughout most of the survey's history have been caused by computer viruses—but almost all respondents say they have anti-virus software and that software has gotten better and better over time. Anti-virus vendors have gotten faster at reacting to new virus threats and

© 2007 by Computer Security Institute. All rights reserved.

Figure 16. Dollar Amount Losses by Type of Attack



Total Losses for 2007 = $66,930,950

(Numbers above do not equal total due to rounding.)

CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 194 Respondents

© 2007 by Computer Security Institute. All rights reserved.

the infrastructure of anti-virus solutions has gotten faster at distributing new virus definition files.

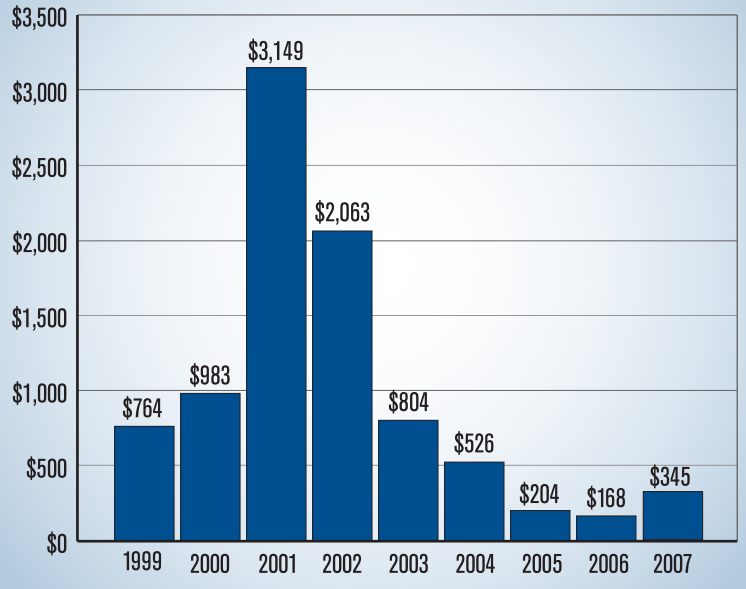
So whereas a virus such as "ILOVEYOU" could wreak relative havoc in 2000, causing estimates that 45 million computers were affected in a single day, more recent years (including last year) have been relatively calm. Organizations have furthermore gained considerably in their ability to deflect run-of-the-mill attacks on their networks by using well-tuned firewalls at points where their networks connect to the Internet.

While there has been increasing (and justifiable) media attention turned toward organizations that have mishandled and lost customer and client private data, the furor over some of the more dramatic data losses has masked the fact that most of the millions of businesses in the United States either haven't lost such data or haven't complied with laws requiring them to confess their errors. Even when an organization's data loss is publicized, the actual cost to the company isn't necessarily catastrophic. Whatever the costs of identity theft, most of them are not paid by the company that lost the data in the first place, so it's even possible that cybercrime losses could be shooting upward due to costs placed on consumers while enterprise losses were falling.

Notwithstanding all the points made above, security professionals observing the state of the "hacker" underworld have long been very concerned about several significant factors likely to change the face of cybercrime within organizations.

The first of these is the shift toward a "professionalization" of computer crime. This has been much discussed elsewhere and is outside the scope of this report. Suffice it to say, though, that more of the perpetrators of current computer crime are motivated by money, not bragging rights.

Figure 17. Average Losses Per Respondent
In Thousands of Dollars



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

Additionally, the security measures that organization have taken against their attackers, such as the anti-virus and firewall components discussed above, are fundamentally imperfect. This is because much of the defensive posture of a typical organization relies on technologies that attempt to identify known, broadly distributed attacks that have easily recognizable "patterns" in them.

This approach of looking for the "signatures" of known threats can often be highly practical, but over time developers of malware (viruses and their ilk) have been gradually increasing the

© 2007 by Computer Security Institute. All rights reserved.

sophistication of their methods and are arriving at points where it is possible to bypass an anti-virus package more or less at will, at least within a limited time frame.

Malware authors have gotten more sophisticated and, at the same time, computer operating systems and software environments have gotten exponentially more complex. While sophistication serves the criminal, however, complexity is the enemy of security (indeed, this phrase is something of an old chestnut among security professionals). It is exceedingly difficult to look at a current-generation desktop computer (whether it's running Microsoft's Windows, Apple's OSX, or any of the variants of Unix and Linux) and reliably tell whether it's been compromised. If a well-known and less sophisticated attack has been made, standard defenses will detect it. But the tide is shifting to sneakier, stealthier attacks.

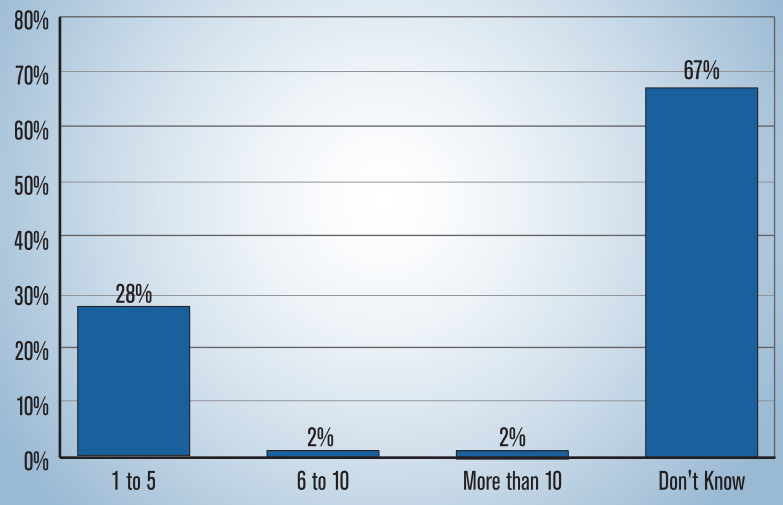
Many observers have been expecting "targeted attacks" to increase, but have seen relatively little direct evidence of them prior to this year.

In the news of recent months, we've witnessed the detection of actual targeted attacks in the wild. In mid-July 2007, *The Washington Post* reported attacks on "computers belonging to the U.S. government, contractors and companies in the transportation industry were hit" in an attack earlier that month. From an April 18, 2007 article at DarkReading.com:

> Such narrowly targeted attacks are becoming more popular than ever, according to a new report issued today by MessageLabs. The messaging security company says it identified 716 e-mails in 249 targeted attacks last month. The attacks targeted 263 different domains, belonging to 216 different customers.

Figure 18. Percentage of Organizations That Experienced Targeted Attacks

(Numbers do not add up to 100% due to rounding.)



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 252 Respondents

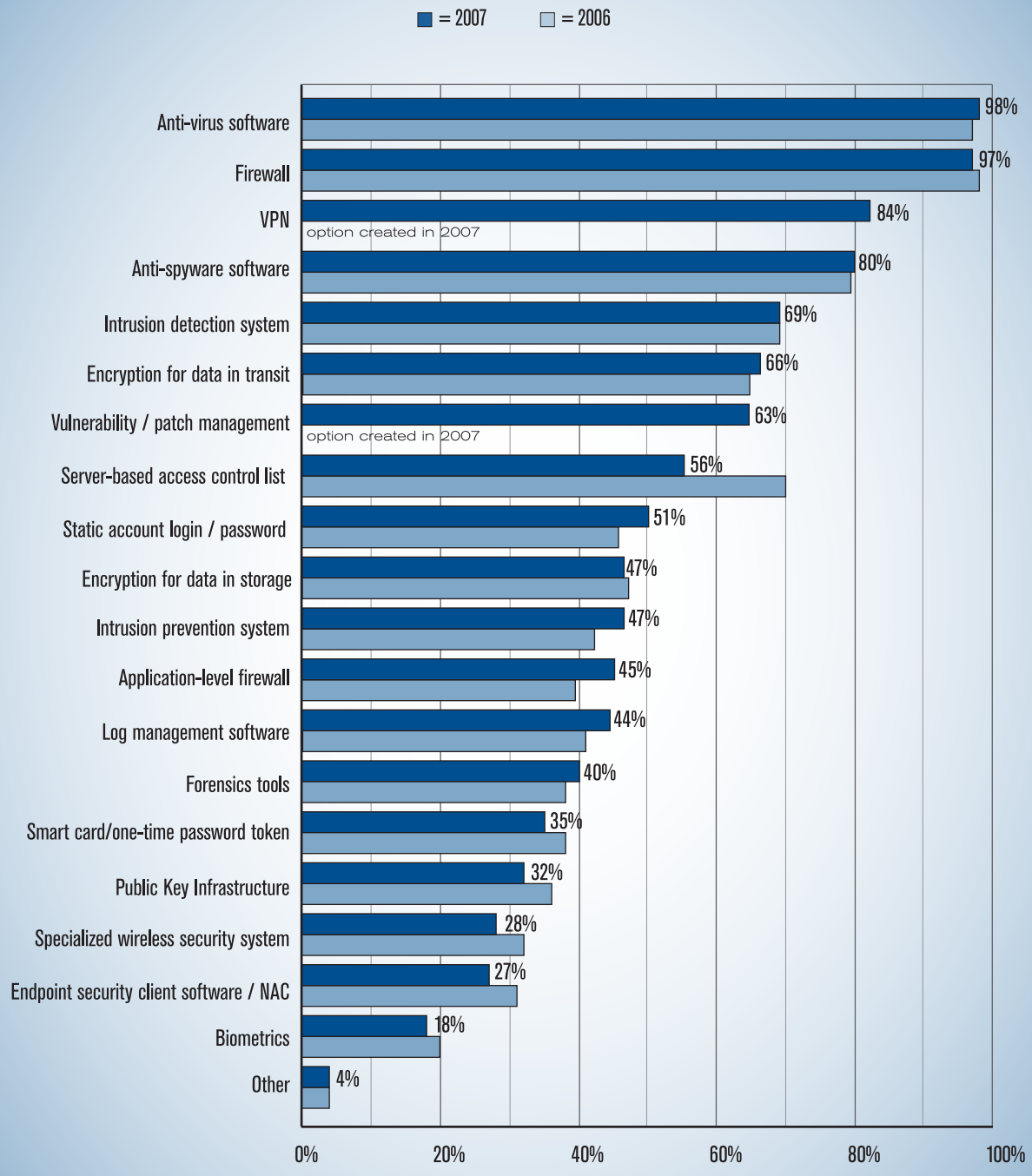
In this year's survey we asked about targeted attacks (**figure 18**), using a fairly broad definition where a "targeted attack" was understood to mean a malware attack aimed exclusively at your organization or at organizations within a small subset of the general business population such as within a specific area or industry.

Very close to one-third (32 percent) of those who answered the question about targeted attacks said that at least some of those incidents involved targeted attacks under this definition. It is probably more accurate to compare the number reporting some number of targeted attacks to the number of respondents reporting security incidents overall (asked in the prior question), in which case the result drops to 18 percent. This still strikes the author as an important and unsettling finding. Five years ago, the notion of targeted malware was hypothetical; today it is a significant reality.

© 2007 by Computer Security Institute. All rights reserved.

Figure 19. Security Technologies Used

By Percent of Respondents



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

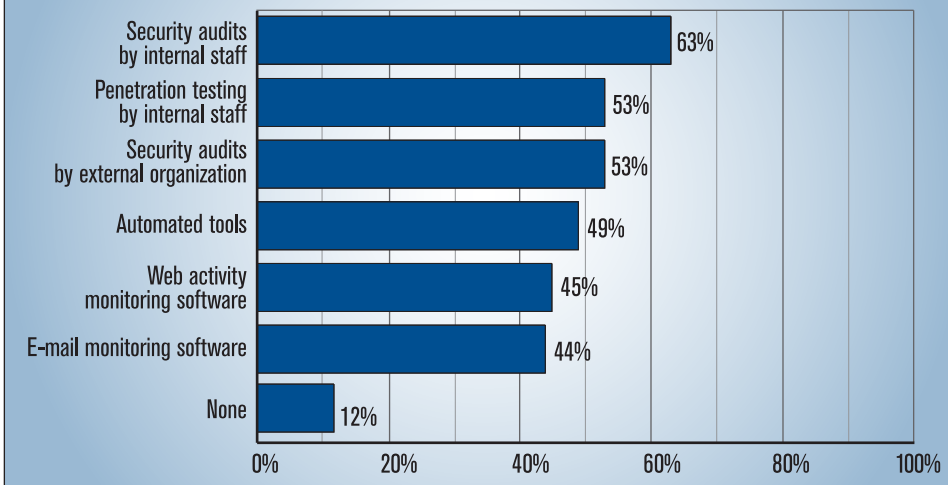
2007: 484 Respondents
2006: 616 Respondents

© 2007 by Computer Security Institute. All rights reserved.

Targeted attacks are much harder to detect than conventional mass attacks. This no doubt means that many penetrations of network defenses will go unnoticed either for a very long time or, practically speaking, forever. That said, the CSI survey asks about attacks in two different ways, first in terms of whether they have occurred at all, and second in terms of financial damages to the organizations where the respondents work. If targeted attacks are more successful and are perpetrated by criminals motivated by financial gain, then we'll expect to see a great many of these crimes noticed when organizations actually lose money to these attacks.

Figure 20. Techniques Used to Evaluate Effectiveness of Security Technology

By Percent of Respondents



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 475 Respondents

As already shown, average losses are greater this year. Whether these losses are directly attributable to an increase in targeted attacks is impossible to say, given the current data set. Nevertheless, there are clear suggestions in the data that the nature of attacks and resultant losses is shifting.

Financial fraud overtook virus attacks as the source of the greatest financial losses. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. If separate categories concerned with the loss of customer and proprietary data are lumped together, however, then that combined category would be the second worse cause of financial loss. Taking financial fraud and data loss categories together, they account for nearly half of the overall reported losses.

The categories concerning data loss and the theft of mobile devices were separated out for the first time this year. Theft of proprietary data from mobile devices tallied to $2,345,000, while theft of customer data from mobile devices came to $2,203,000. The cost of the stolen mobile hardware itself was reported at $3,881,150, which is interesting in that it is not as much lower a figure than the estimated costs of data loss as might be expected, given that the conventional wisdom is that the cost of the hardware is inconsequential when held up alongside the loss of the data stored on the hardware. Apparently the hardware loss adds up fairly quickly as well.

Security Technologies Used

As in previous years, respondents were asked to identify the types of security technology used by their organizations (**figure 19**, page 18). As in almost all other years, organizations use the sorts of technologies you'd expect them to, with nearly all reporting the use of firewalls and anti-virus software, and 80 percent reporting that they use anti-spyware tools (it was 79 percent last year,

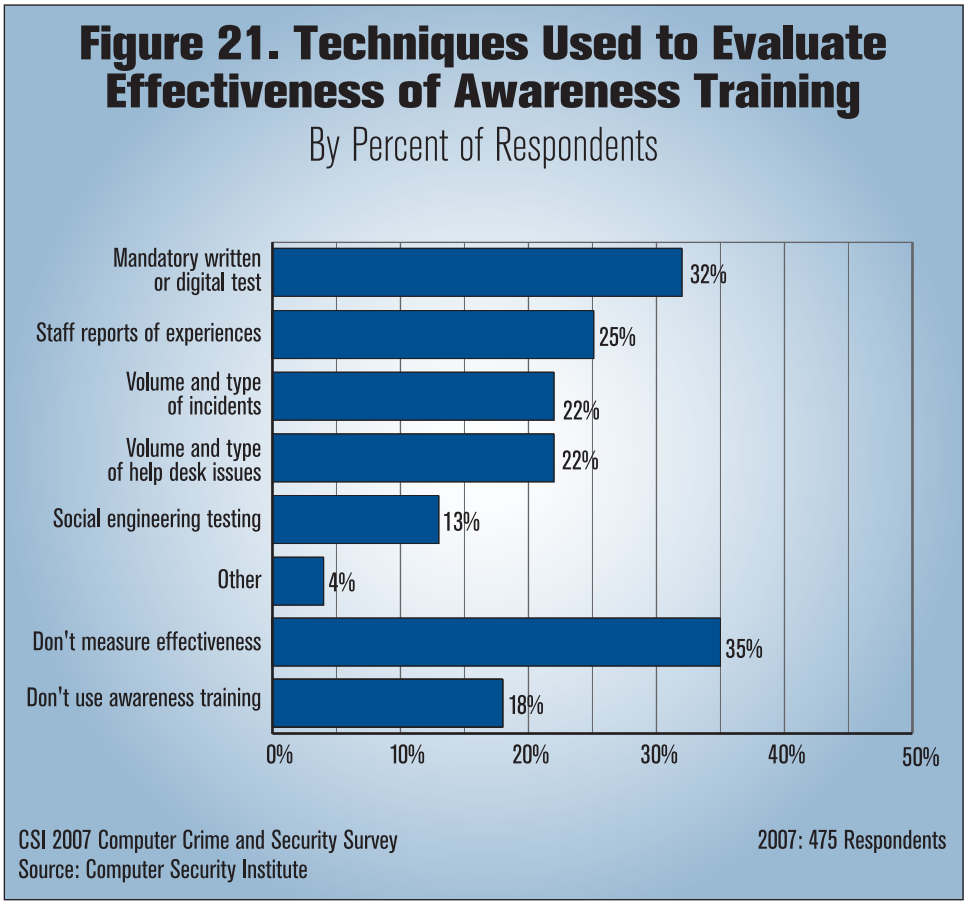
© 2007 by Computer Security Institute. All rights reserved.

the first year we asked). We asked whether organizations are using VPNs for the first time this year, with 84 percent reporting that they did. After ratcheting up to 20 percent from 15 percent in the 2005 survey, the biometric category settled back to 18 percent. Most of us are apparently as far away as ever from having our retinas scanned on a regular basis.

Security Audits and Security Awareness Training

Implementing security measures is one thing; verifying that they are properly in place and effective on an ongoing basis is another. We asked: "Which techniques does your organization use to assist in the evaluation of the effectiveness of its information security?" **Figure 20** (page 19) illustrates that 63 percent of 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 as it has been for the prior two years (the question was introduced in 2005). The percentage, though, is markedly lower than it was in the 2005 and 2006, when it was 82 and 87 percent respectively. It's unclear what this drop means, as the number reporting external audits didn't rise accordingly, though adding a response for "internal penetration testing" may have siphoned off some of the previous "internal audit" responses. The use of the other techniques—penetration testing, automated tools, security audits by external organizations, e-mail monitoring software and Web activity monitoring software—is clearly also prevalent.

For the first time this year the survey also asked about measures organizations had adopted to gauge the effectiveness of their security awareness training programs. **Figure 21** shows, among other things, that 18 percent of respondents don't use awareness training, implying that 4 out of 5 respondent organizations do in fact engage in training their employees about security risks and appropriate handling of sensitive data.



Although a strong majority perform this kind of training, many of the respondent organizations (35 percent) make no effort to measure the effect of this training on the organization. A quarter of them learn anecdotally from reported staff experiences; roughly one third (32 percent) administer tests to see whether their lessons have

© 2007 by Computer Security Institute. All rights reserved.

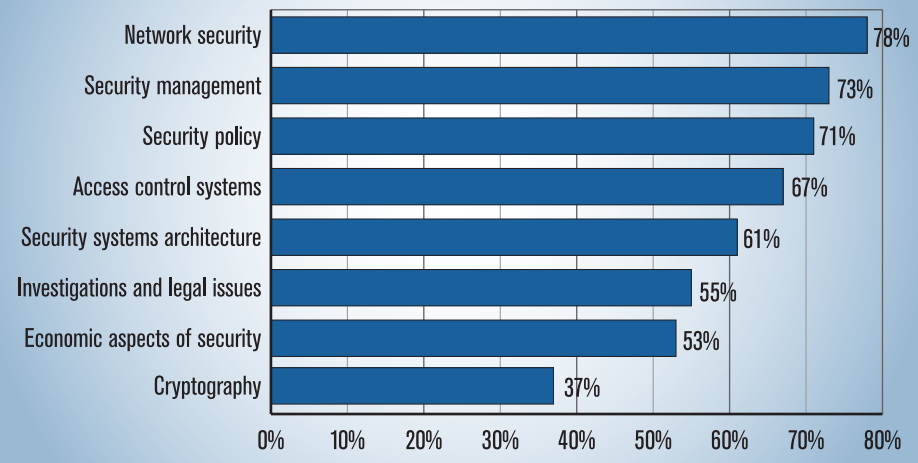
taken hold. Only about one in ten (13 percent) of the respondents say they test the effectiveness of the training by checking whether employees can detect internally-generated social engineering attacks.

Participants were also asked to rate the importance of several security awareness training topics to their organizations. **Figure 22** shows the percentages of respondents indicating that security awareness was important (as measured by ratings of 5 or above on 7-point scale) in the various areas of security. As was the case last year, network security (78 percent), security management (73 percent) and security policy (71 percent) took top rankings, though in a different order than last year.

On the whole, these numbers are very similar to those seen in last year's survey, which in contrast showed a jump in the importance of several areas. Last year, security architecture jumped 34 percent over the prior year, for example. We speculated at the time that the increasing complexity of enterprise information systems and information security systems is driving the

Figure 22. Importance of Security Awareness Training

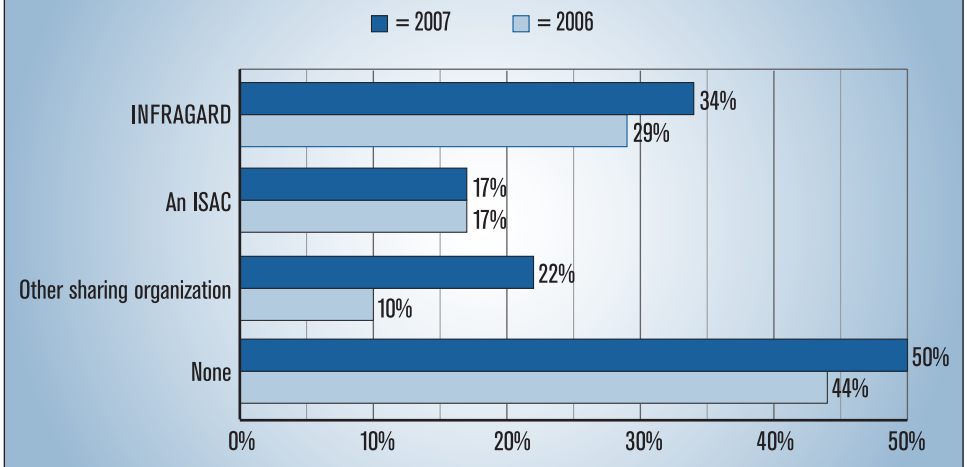
By Percent of Respondents Identifying as Important



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 486 Respondents

Figure 23. Percentage That Belong to an Information Sharing Organization

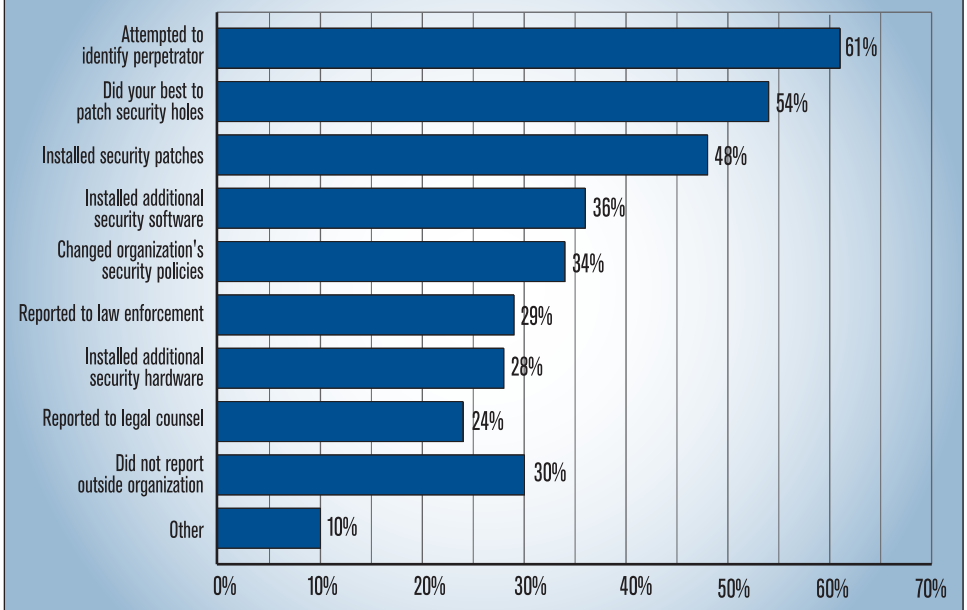


CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 424 Respondents

© 2007 by Computer Security Institute. All rights reserved.

Figure 24. Actions Taken Following an Incident
By Percent of Respondents



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 274 Respondents

respondents to recognize the importance of security systems architecture training—but perhaps a plateau has been achieved. The responses indicate an overall steady and substantial 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. 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 23** (page 21). Some 34 percent of respondents indicated that their organizations belong to INFRAGARD, up 5 percent from last year, while 17 percent belong to an ISAC, and 22 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. While the "other" category rose significantly from last year, it's still below the percentage from the year before. Overall, there's certainly a significant level of involvement with information sharing organizations, but there's no clear surge in growth of membership in such groups.

Beyond inquiring about membership in information sharing organizations, respondents were asked whether they shared information on computer intrusions with law enforcement and legal counsel, and more generally what their actions were following a computer intrusion (**figure 24**). This year, the question's array of possible responses was broadened to include several new answers.

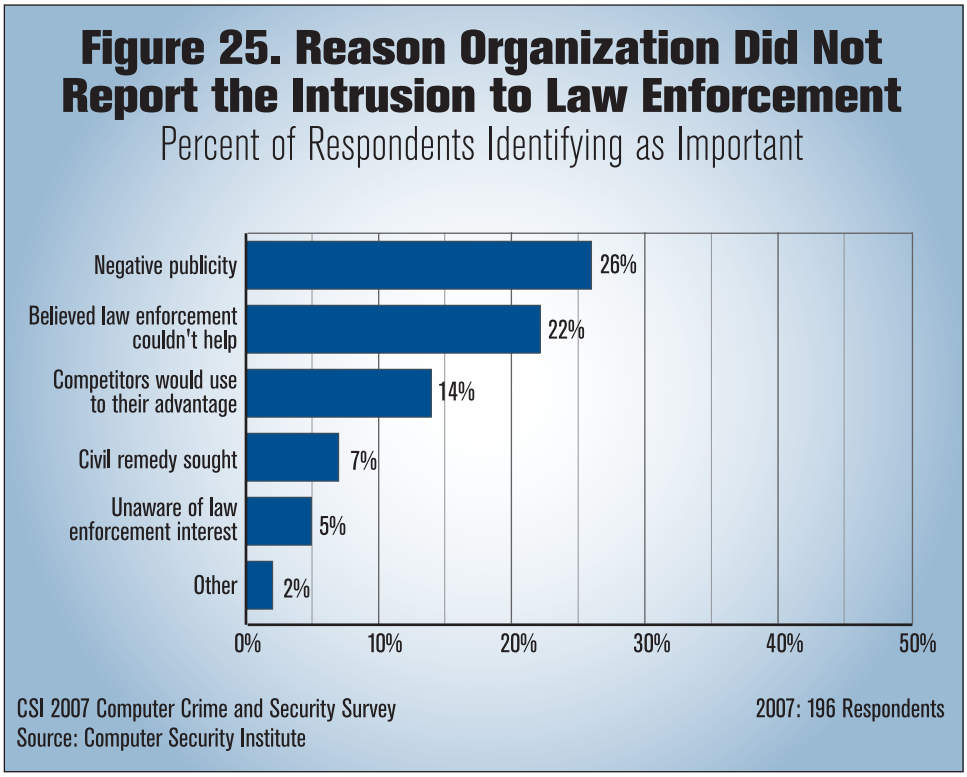
Perhaps the most interesting finding among these new answers is that only about one-third of respondents said that their security policies didn't change in the wake of incidents, suggesting that there was no need to create or amend policy, but rather that the policies had been broken or that inside, policy-governed behavior was not a factor in the incident.

© 2007 by Computer Security Institute. All rights reserved.

Among answers that have long been available with this question, one of particular interest has been the percentage that report to law enforcement. This year that percentage reached its highest level (29 percent) since 2003, when 30 percent said they reported the incident to law enforcement. By way of comparison, the highest level for this response in the survey's history was 36 percent, reported in the 2001 survey. In past surveys, corporate legal counsel has never fared well, with respondents saying in 2005 that only 12 percent reported incidents to their internal lawyers. This year that percentage jumped to 24 percent. It's been higher (it peaked at 30 percent in 2001), but this year's jump may indicate that internal legal departments are increasingly part of the information security picture.

Figure 25 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 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. As has always been the case, 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 law enforcement) was the perception that resulting negative publicity would hurt their organization's stock and/or image.[2]

The percentage citing this answer dropped significantly from last year (when it was 28 percent), but this appears to be an effect of changes to the question, specifically that other options were given. As mentioned above, this question is framed as reflecting the level of agreement or disagreement across a seven-point scale. Respondents, however, invariably treated this as a series of yes or no questions. In other words, they either answered "strongly agree" or "strongly disagree" and never chose the more nuanced options in the middle of the scale. Furthermore, it would appear that respondents picked the option relevant to them and didn't necessarily address other options offered for the question. So, to take the most relevant example, if "fear of negative publicity" is considered as a yes or no question in its own right, then the percentage of respondents who answered "yes" for only that portion of the survey is 43 percent, much more in line with last year's percentage and exactly matching the prior year.

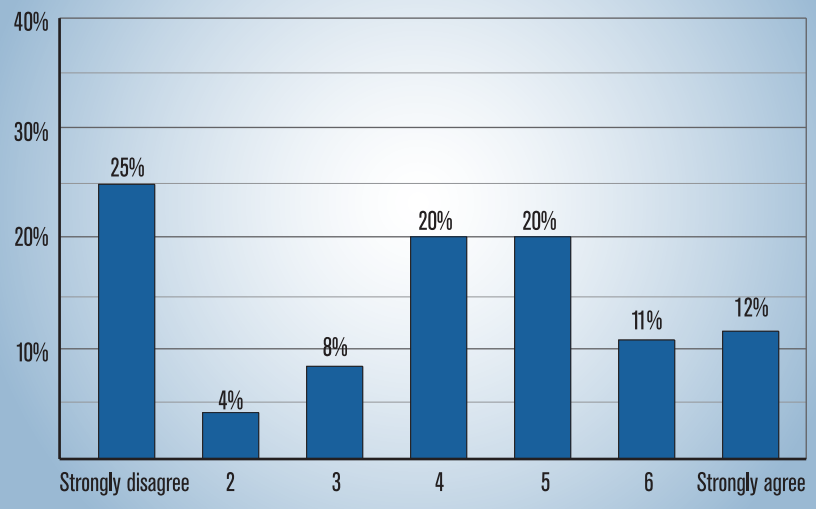


2. *This is consistent with re-cent research by Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou ("The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market,"* Journal of Computer Security, *Vol. 11,No. 3, 2003, pp. 431-448) that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

© 2007 by Computer Security Institute. All rights reserved.

Figure 26: Sarbanes-Oxley Has Improved Organization's Information Security

By Percent of Responses Chosen on a Seven-Point Scale

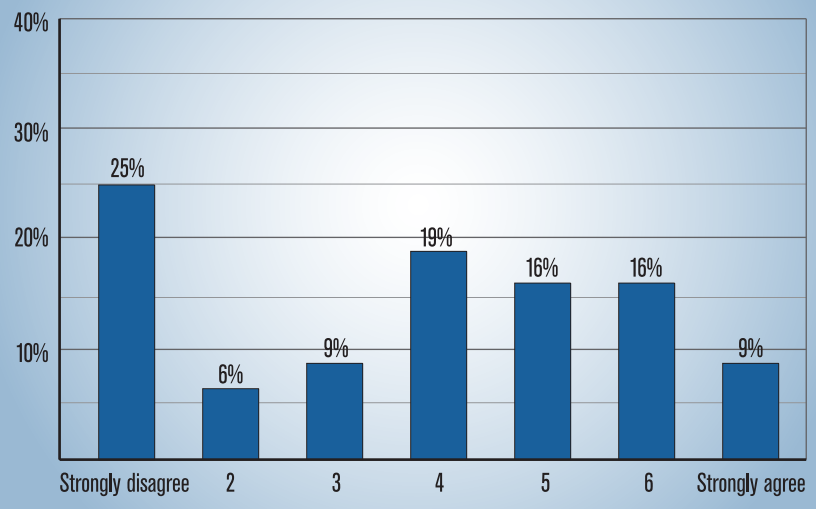


CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 387 Respondents

Figure 27: Sarbanes-Oxley Changed Security Program's Focus to Governance

By Percent of Responses Chosen on a Seven-Point Scale



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 387 Respondents

The most interesting finding from the question this year was the strong response to a newly added option: "Did not believe that law enforcement could help in the matter," which garnered 22 percent overall agreement. It's hard to say whether this reflects cynicism about law enforcement effectiveness or simply shows realistic assessments of what law enforcement has the resources to tackle (there are plenty of crimes in all walks of life that go unreported for precisely this reason—a police officer witnessing a jaywalker may cite the offender, but no bystander witnessing jaywalking in the absence of a police officer bothers to pick up the phone).

There is something of a dark underbelly to this question as well, lurking in the "other" category, where respondents are asked to specify their reasons. There weren't a great many responses where further information was filled in, and some of the reasons were as straightforward as saying that incidents were traced back to relatively minor failures to adhere to stated security policies. But in more than one other instance national security was cited as a reason why the matter was not reported and in another case the claim was that upper management simply refused to believe the severity of the breach.

© 2007 by Computer Security Institute. All rights reserved.

Certainly no firm conclusions can be built atop these very few responses, but they're nevertheless suggestive.

Effect of Sarbanes–Oxley Act

Since 2004 we've asked questions about the effect of the Sarbanes-Oxley Act on the information security activities. Overall, the results have indicated that the Act has had a definite impact, though it has certainly not changed the entire face of security management. This year, 43 percent of respondents agreed with the statement "Compliance with the Sarbanes–Oxley Act has improved my organization's information security" (**figure 26**) It's worth noting, on the other hand, that a full quarter of the respondents strongly disagreed with the statement.

A second question regarding Sarbanes–Oxley queried respondents on their reaction to the statement "The Sarbanes–Oxley Act has changed the focus of information security in my organization from technology to one of corporate governance" (**figure 27**). Here 41 percent of respondents found themselves in agreement, a result not dissimilar from that of the previous question. Again, however, a full quarter of the respondents chose the strongest option for disagreement with the statement.

General Concerns

Finally, this year's survey also included 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?" In order to get a better view of the key topics across the breadth of these responses, they were categorized into basic topic areas, such as "data protection" and "phishing." There are, of course, some answers that might be interpreted in different categories than were decided upon here, but generally speaking, the topics broke into three levels of concern. Mentioned by 49 respondents apiece, the categories of "data protection" and "legal issues and compliance" were clearly areas of top concern for our respondents. This is completely consistent with last year, when these two categories also led the field.

Given both the media scrutiny of enterprise breaches and the very nature of the assets that computer security is designed to protect, the focus on data protection is hardly surprising. Some industry pundits have on occasion predicted that the focus on compliance as a driving force within the security industry might wane once the first round of audits had been survived. While this may happen, it seems clear that this set of respondents doesn't see compliance issues going away anytime soon.

The next group of concerns, with the number of respondents citing each issue ranging from 27 to 39, had identity and access management as its top issue. This is particularly interesting given that data protection and compliance are very broad issues compared to identity management. It suggests that identity is perhaps the biggest single issue on the radar of enterprise security practitioners. Given that some of the largest vendors (such as Microsoft) and industry groups (such as the Trusted Computing Group) are rolling out products and over-arching protocols to push a new generation of identity management, it makes sense that infosec professionals would be paying attention, but it's also clear that they've positioned identity as a top issue.

The general category of management-related issues (needing to convince upper management of the benefits of strong security, finding appropriate staff, interoperating well with business units, and so on) ranked close behind, followed by awareness training. Also in this grouping of concerns: mobile device concerns (including theft) and the insider threat. It's interesting to note that most of the issues mentioned so far are not, for the most part, technically driven concerns. Implementing hard-drive encryption on the corporate fleet of notebooks is a technical matter, to be sure, but awareness training isn't, nor is regulatory compliance.

A third tier of issues included maintaining customer and healthcare-related privacy (which is, of course, intimately related to the issue of data protection), wireless network security, viruses and similar malware,

© 2007 by Computer Security Institute. All rights reserved.

phishing scams, "bot" networks and rootkits, remote access, endpoint control (NAC), the implementation of security policies, and Web-related attacks. There was a handful of mentions (8) of migration to the new Microsoft Vista operating system. Additionally, 9 respondents specifically mentioned targeted attacks as a key issue for the coming year.

There were many other issues that were mentioned singly or in small numbers, some of which might arguably have been included in some of the groupings above. That said, it's interesting to note that some issues didn't seem to have much traction as top issues: IPv6 migration was mentioned in only one instance; VoIP rated only four inclusions.

Obviously, it's possible to group these issues in other ways and it's useful to think about which elements are more and less related to one another. To the author's way of thinking, specific concern about targeted attacks is different than concern about malware randomly downloaded from a Web site, but it's true that many targeted attacks are delivered using customized malware not unlike its mass-distributed brethren.

CONCLUDING COMMENTS

In recent years, this survey has seemed to suggest that—while consumer-focused crime such as phishing might be skyrocketing—security was improving within enterprises. While it was satisfying to see security professionals estimating that their losses were down, it also seemed clear that the trend couldn't continue indefinitely, especially not given that several factors observable within the online world pointed toward troubled times ahead. Networks and operating systems have become more complicated in the past few years; malware developers have clearly been developing and trying out various components that, as they are combined, will create attacks that are more dangerous and more difficult to detect; and the IT sector is retooling its applications using service-oriented architectures that—while they may produce a Web 2.0 economy—will also create a mother lode of new vulnerabilities that will be very difficult to contain.

This year, then, respondents tell us that they lost more money to cybercrime on average than last year. It is very difficult to predict whether that signals increasing losses in the years ahead, in no small measure because information security professionals won't sit idly by. They will react to shore up their defenses.

Nevertheless, the stakes are high and the outlook isn't necessarily comforting. 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. We have already witnessed some of the costs that are incurred when services are interrupted and data stolen or misused. We know, furthermore, that cybercrime and the attendant threat of identity theft 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.

In the past, the struggle has been cast as one between security professionals and the criminals who attack their networks. Now, the picture is more complicated. Criminals attack both enterprise networks and steal customer data. They use this data to then attack individual consumers. Meanwhile, the high-tech world as a whole seems poised to radically retool identity management—a move that may very well curtail crime. It will be much harder to use many network assets to commit crimes because users will have to identify themselves unequivocally, using means more reliable than an e-mail address. The infractions they then commit will be easily tracked back to real-world names and addresses.

© 2007 by Computer Security Institute. All rights reserved.

Tighter identity management (particularly with appropriate privacy protections) might be a game-changing gambit for a corporation to undertake, but many corporations are also undertaking overhauls of their line-of-business applications so that they are Web-facing, exposing old, previously internal systems to the world's hackers.

Where will the balance between vulnerabilities and safeguards lie in a year's time? If no more than the status quo of firewalls and anti-virus are maintained, it's hard to foresee anything other than the erosion of enterprise security. Time, of course, will tell.

Meanwhile, regardless of the threats and the opportunities, those responsible for computer security have to make their case within their respective organizations: security professionals are increasingly being asked to develop 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.

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 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 CSI hopes to be valuable additions to this required knowledge base. CSI's 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.

A NOTE FROM CSI DIRECTOR ROBERT RICHARDSON

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

Long-time readers of the survey will surely have noticed that "FBI" did not appear in the title this year. While we've been happy to acknowledge the FBI, under the auspices of the Bureau's San Francisco Computer Intrusion Squad, the survey has clearly gained a national scope and significance over the years. In moving to embrace this larger scale, CSI continues to maintain contacts with agents both in the headquarters offices and in many major cities where the Bureau has computer crime squads. Furthermore, we've become increasingly engaged with the efforts of InfraGard, the FBI-sponsored coalition aimed at extending information sharing between private industry and the government.

Nevertheless, both CSI and our contacts at the FBI felt it was important to make it clear that this survey is an effort of the private sector and not a government research product. CSI has no contractual or financial relationship with the FBI. CSI funds the project and is solely responsible for the results.

Finally, the editorial heavy lifting involved in preparing this report for production, along with the production itself, is handled with efficiency and grace by CSI Editor Sara Peters, to whom I offer a special thank you, particularly for her patience when the writing process was slow.

Regarding Methodology

The survey was distributed to 5,000 information security practitioners in the United States in early January 2007, both in a hardcopy, first-class mailing and in a Web e-mail distribution. Two subsequent mailings and e-mailings followed at approximately

© 2007 by Computer Security Institute. All rights reserved.

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 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. 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 special permission: contact Robert Richardson at rrichardson@cmp.com.

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

© 2007 by Computer Security Institute. All rights reserved.

CSI

PRACTICAL INSIGHTS FROM THE BEST MINDS IN SECURITY

The perimeter "vanished" several years ago, but endpoint controls are only now shaping up. Your colleagues are trying several approaches, and you need to know how they're faring.

Networks are incorporating a new "identity layer" that will *redefine* security. You need a rational plan for adapting your access control systems.

Web 2.0 sounds pretty exciting–if you're a hacker. Otherwise, you need to connect with your software developers, and soon.

You can't do business without compliance to several legislative requirements at once. You need real-world mappings of one acronym to another, guidelines to measure your organization against the right benchmarks, and access to the sure hands that have led several Fortune 500 companies over the hurdles.

CSI delivers a relentlessly business-focused view of enterprise information security. As security professionals grapple with these challenges, CSI is there to provide depth and insight, energy and inspiration from each of these intersecting points.

CSI publications and special reports delve deeper into the news with interpretive analysis to help security professionals decide for themselves what's real, what's hype and what's right for their organization.

With an ongoing series of regional events culminating in an annual conference each autumn, CSI provides the inside track to top educators and innovative vendors in a thought-provoking, stimulating environment.

Learn who and what's on tap for CSI 2007–Nov. 3 to 9 in Arlington, Va.–at **CSIAnnual.com.** Learn more about CSI at **GoCSI.com.** Catch up with security news at **GoCSI.com/blog.**