EIGHTH ANNUAL

2003

CSI/FBI

COMPUTER CRIME AND SECURITY SURVEY

CSI
COMPUTER
SECURITY
INSTITUTE

By Robert Richardson

The Computer Crime and Security Survey is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The survey, now in its eighth year, has the distinction of being the longest-running survey in the information security field. As in previous years, the survey paints a compelling portrait of just how often crime occurs on computer networks and just how expensive such crime can be.

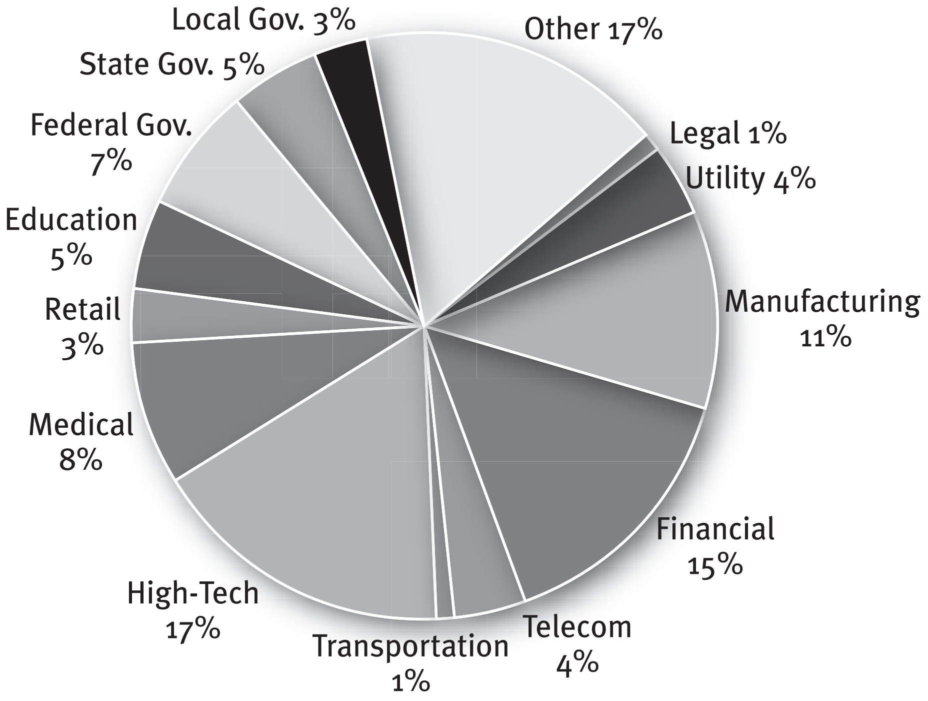
Based on the responses of 530 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the 2003 findings once again show that there is no shortage of attacks, but suggest this year that the severity and cost of these attacks has trended downward for the first time since 1999.

Despite the lower number for aggregate financial losses among survey respondents, the most important conclusion one must draw from the survey remains that the risk of cyber attacks continues to be high. Even organizations that have deployed a wide range of security technologies can fall victim to significant losses. Furthermore, the percentage of these incidents that are reported to law enforcement agencies remains low. So attackers may reasonably infer that the odds against their being caught and prosecuted remain strongly in their favor.

ABOUT THE RESPONDENTS

Those answering the survey represent companies and organizations across the spectrum of modern life. Some 17 percent are from high-tech companies; an additional 15 percent come from the financial sector. Government agencies make up, in total, about 15 percent of the survey responses. Thus, about half of the responses come from quarters where it's hardly surprising that computer security would be an important concern. This tracks closely to previous years, although those answering "Other" rose to 17 percent

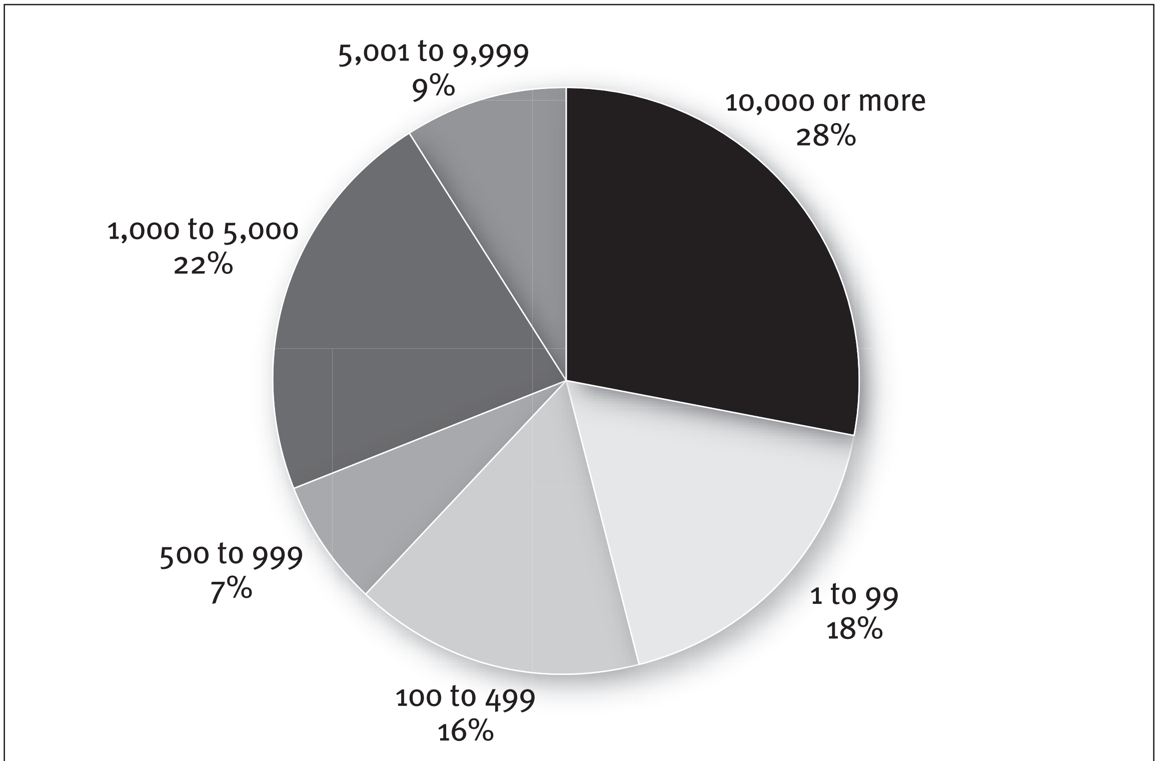
Respondents by Industry Sector



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 530 Respondents/100%
Totals 101% due to rounding.

Respondents by Number of Employees



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 528 Respondents/99%

from just 5 percent in the 2002 survey.

More than half of the organizations represented in the survey employ more than 1,000 employees, with approximately one-quarter of the respondents (28 percent) reporting more than 10,000 employees. This roughly corresponds to revenues: 34 percent report more than $1 billion in annual revenues.

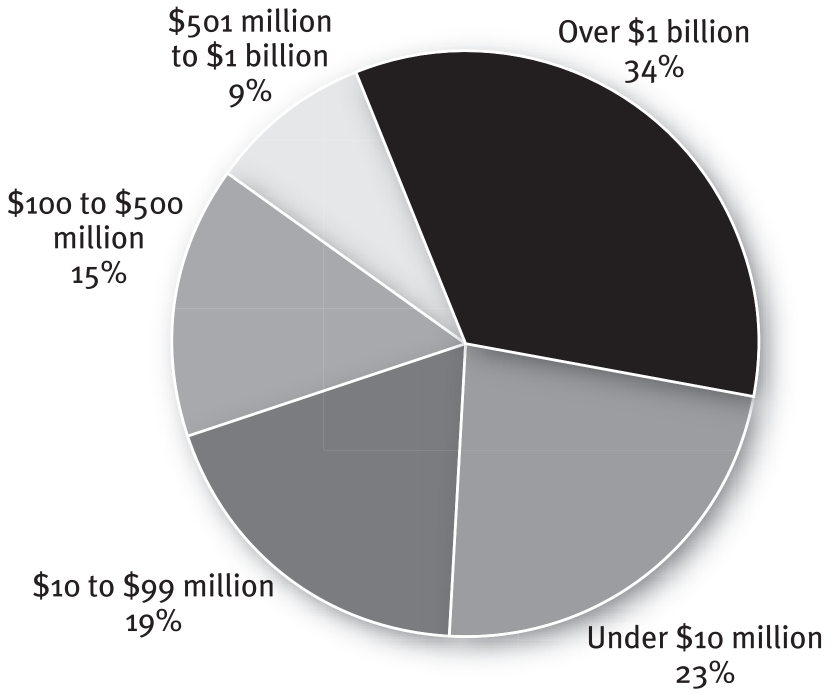
While this clearly shows that large-scale corporate America is well represented both among the CSI membership and among survey respondents, it is not the case that the experiences of small business find no voice in the survey. In fact, 18 percent of respondents work at organizations with 99 or fewer employees and 23 percent work at organizations reporting less than $10 million in annual revenues.

Those actually answering the survey questions are, not surprisingly, security professionals. They are, furthermore, self-selecting and one presumes are more likely to be sensitive to security incidents than are those who are not affiliated with professional organizations such as CSI. These are people who are paying attention to computer crime and who have a direct interest in stopping it.

SURVEY HIGHLIGHTS

While the percentage of respondents reporting some form of unauthorized computer use remained approximately the same as in previous years, the financial losses reported for these losses plummeted. Fifty-six percent of respondents reported unauthorized use, compared to 60 percent last year (and compared to an average of 59 percent over the previous seven years of the survey). The total annual losses reported in the 2003 survey were $201,797,340, a figure that is down 56 percent from the high-water mark of $455 million reported last year. It should be noted, though, that this figure is in line with figures reported prior to 2001. Additionally, it is important to remember that this figure is simply the total losses reported by a specific number of organizations (251 of them)

Respondents by Gross Income



CSI/FBI 2003 Computer Crime and Security Survey 2003: 393 respondents /74%
Source: Computer Security Institute

and is not any kind of more broadly extrapolated total.

OTHER KEY FINDINGS

❒ The overall number of significant incidents remained roughly the same as last year, despite the drop in financial losses.

❒ As in prior years, theft of proprietary information caused the greatest financial loss ($70,195,900 was lost, with the average reported loss being approximately $2.7 million).

❒ In a shift from previous years, the second most expensive computer crime among survey respondents was denial of service, with a cost of $65,643,300.

❒ Losses reported for financial fraud were drastically lower, at $10,186,400. This compares to nearly $116 million reported last year.

❒ As in previous years, virus incidents (82 percent) and insider abuse of network access (80 percent) were the most cited forms of attack or abuse.

❒ Respondents again weighed in strongly opposed to the idea of hiring reformed hackers (68 percent were against).

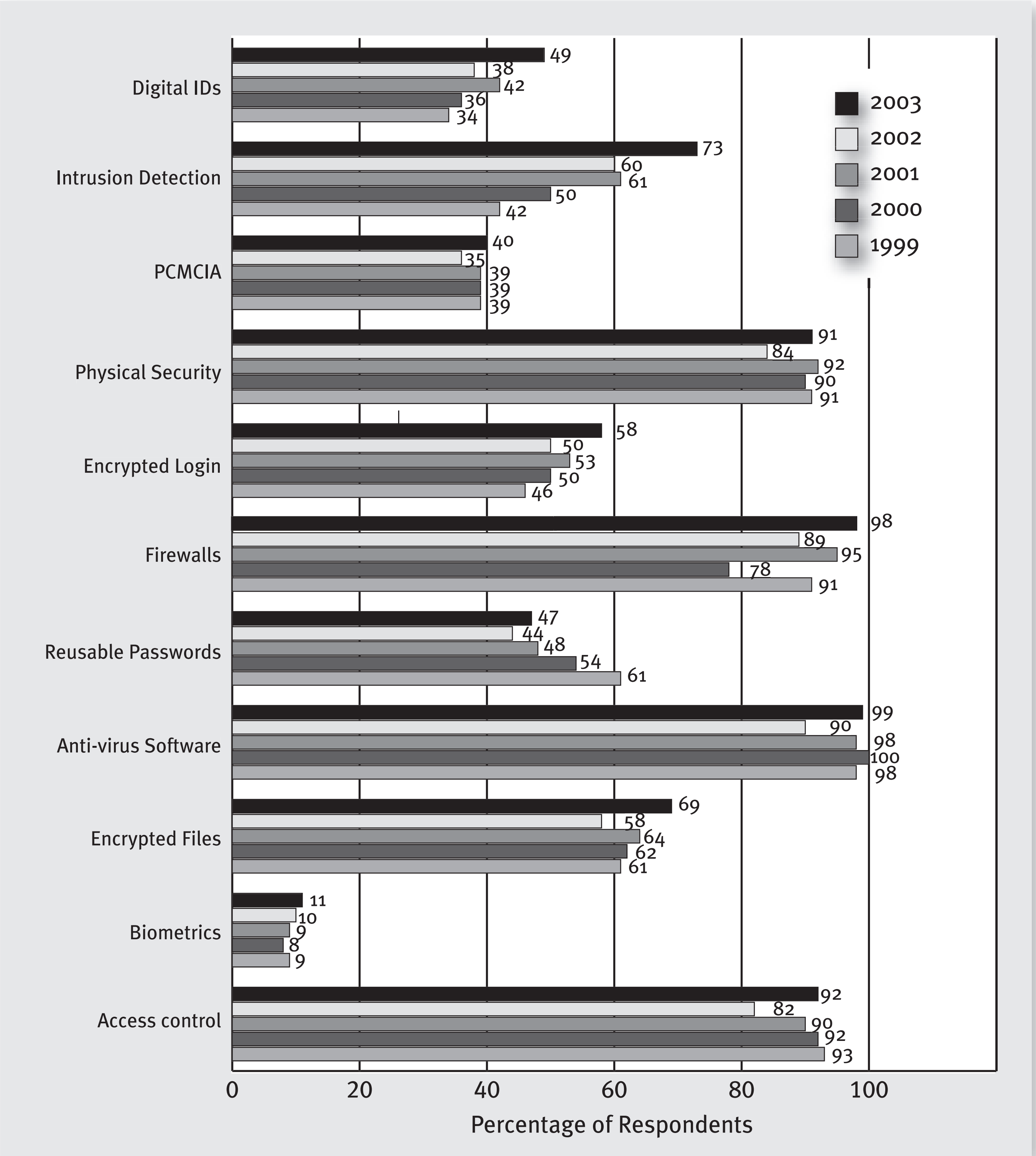
❒ The percentage of those who reported suffering incidents in the prior year who said they reported those incidents to law enforcement remained low (30 percent).

SECURITY TECHNOLOGIES USED

For the sixth consecutive year, survey takers were asked what kind of security technologies they had employed to protect their organizations. Though not all questions on the survey are answered by all respondents, the question that queries the use of various sorts of technology is answered by 99 percent (525 of 530) of the respondents.

Virtually all organizations use anti-virus software (99 percent) and firewalls (98 percent). As one might expect, most (91 percent) employ some kind of physical security to protect their computer and information assets and most employ some measure of access control (92 percent).

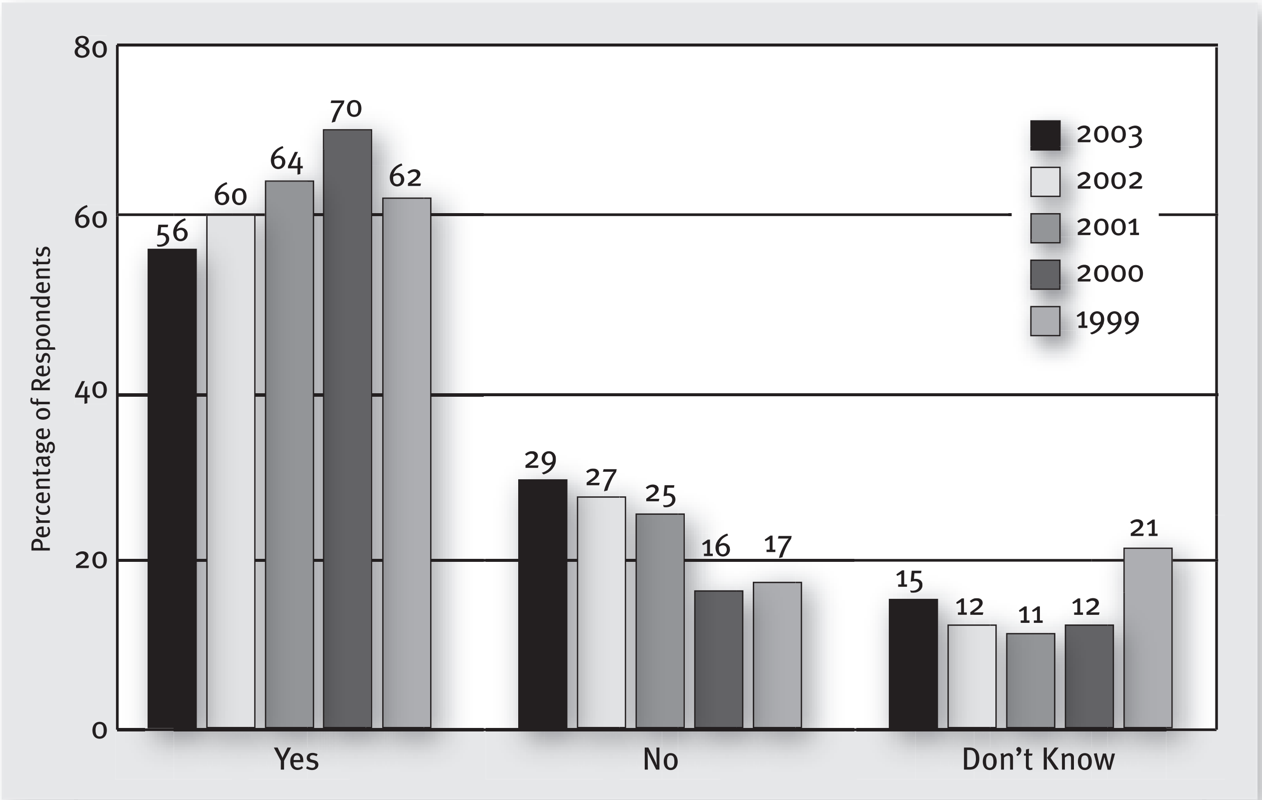
Security Technologies Used



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 525 Respondents/99%
2002: 500 Respondents/99%
2001: 530 Respondents/99%
2000: 629 Respondents/97%
1999: 501 Respondents/96%

Unauthorized Use of Computer Systems Within the Last 12 Months



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 524 Respondents/99%
2002: 481 Respondents/96%
2001: 532 Respondents/99.6%
2000: 585 Respondents/91%
1999: 512 Respondents/98%

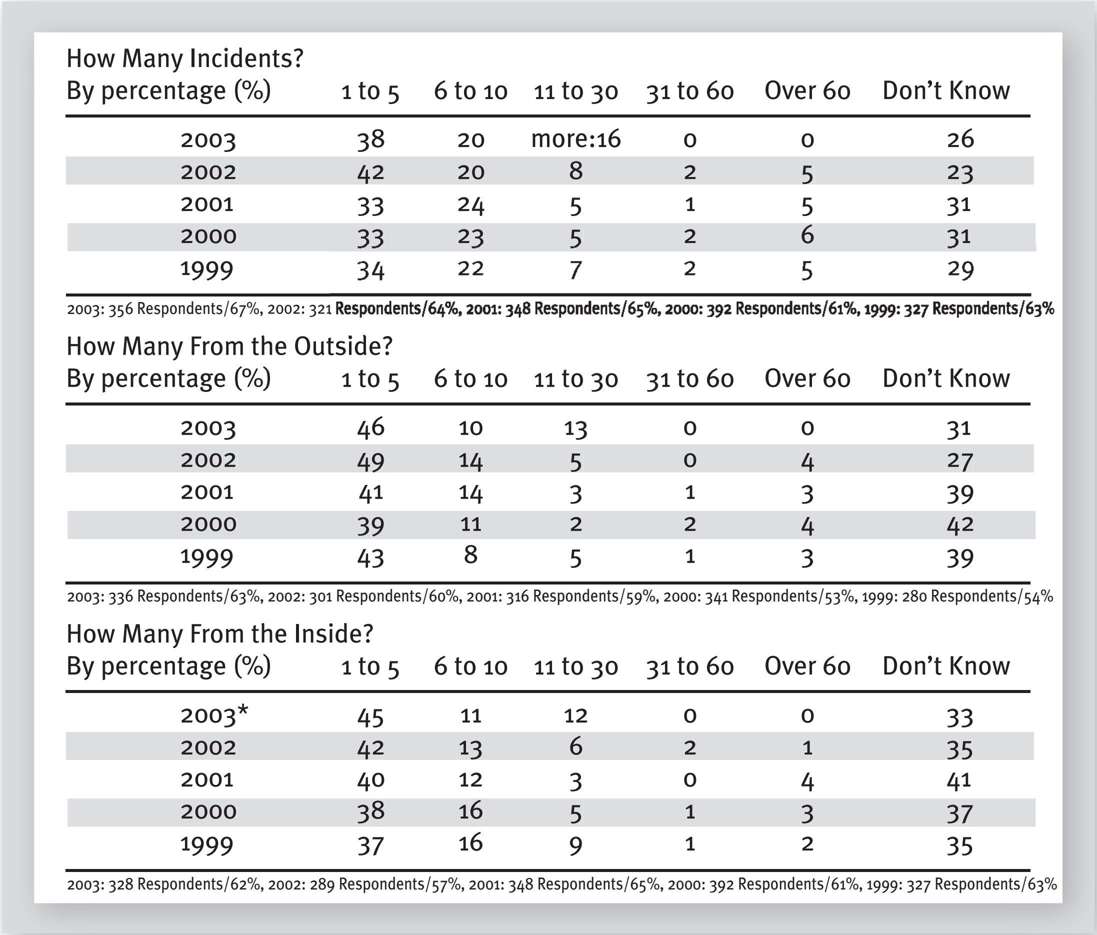
These last two categories are perhaps an appropriate moment to say something about the nature of these sorts of responses. The survey itself is deliberately kept very short and has been left largely the same over its eight-year lifespan (this in the interest of preserving trend information). Thus, respondents are asked to interpret various possible answers on the survey according to their own understanding of the security industry and its terminology. For the most part, this is a sensible approach—most of the terminology within the industry is sufficiently settled that there isn't much question about what it means when the survey asks, for instance, whether firewalls are in use. There isn't much debate about what a firewall is.

In the case of physical security, though, the term is arguably overly broad. Some respondents may interpret this question to be asking simply whether the office premise as a whole is locked during the off hours. Others may quite justifiably interpret the question to be asking whether there are specific measures (special alarms or locked areas) designed to protect computer and network assets.

Perhaps the most interesting aspect of this particular finding, then, is that almost one in ten organizations do not use any extra physical precautions to protect their computer assets. It is quite possible, in other words, that they do not have server equipment within specially locked rooms or that they do not equip mobile equipment such as notebook computers with locking cables.

While access control as a category is well understood, it makes for a broad question. We would anticipate that any organization that required users to provide passwords for access

How Many Incidents? How Many from Outside? How Many from Inside?



How Many Incidents? By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003	38	20	more:16	0	0	26
2002	42	20	8	2	5	23
2001	33	24	5	1	5	31
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29

2003: 356 Respondents/67%, 2002: 321 **Respondents/64%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%**

How Many From the Outside? By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003	46	10	13	0	0	31
2002	49	14	5	0	4	27
2001	41	14	3	1	3	39
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39

2003: 336 Respondents/63%, 2002: 301 Respondents/60%, 2001: 316 Respondents/59%, 2000: 341 Respondents/53%, 1999: 280 Respondents/54%

How Many From the Inside? By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003*	45	11	12	0	0	33
2002	42	13	6	2	1	35
2001	40	12	3	0	4	41
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35

2003: 328 Respondents/62%, 2002: 289 Respondents/57%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%

*Totals 101% due to rounding

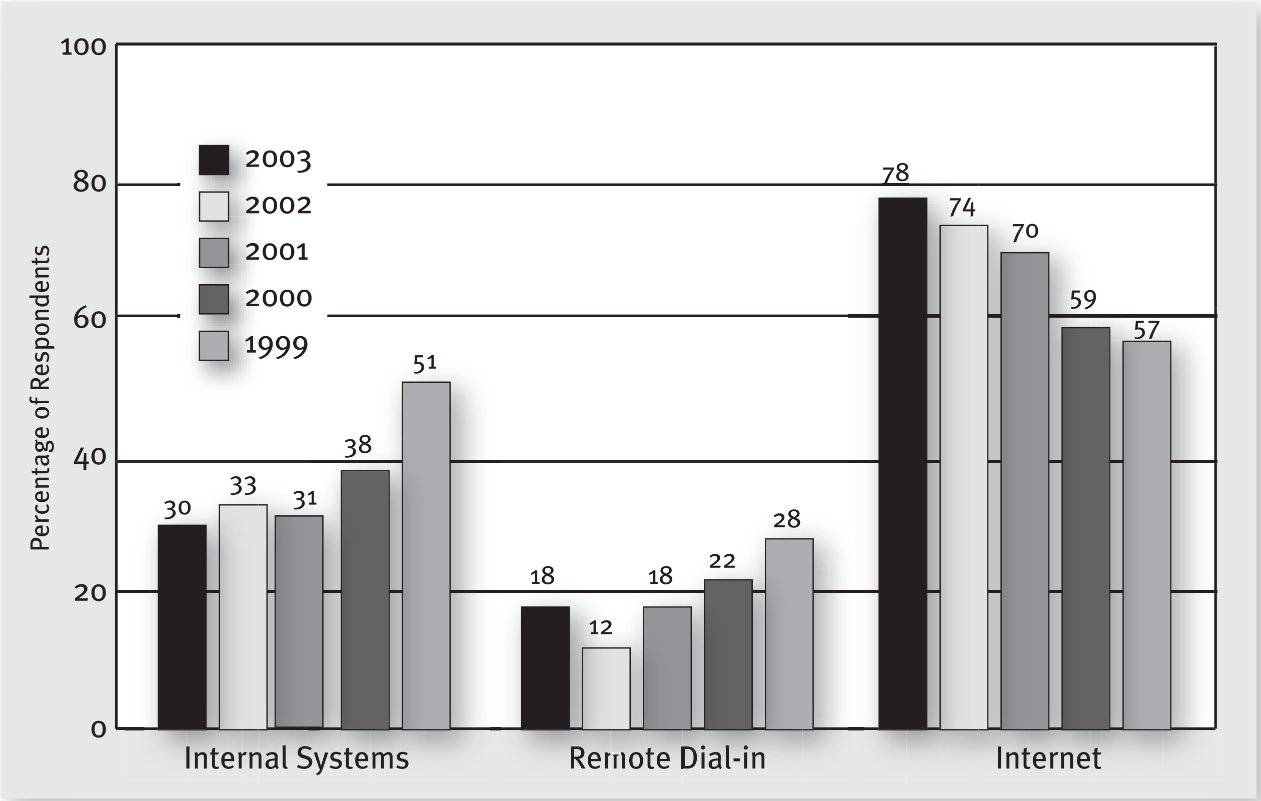
CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

would answer in the affirmative. So, again, it's interesting that 8 percent of respondents say no, they do not employ access control. Of the 48 respondents who said they didn't use access control, only six said they produced revenues in excess of $1 billion, with two of those answering that they used reusable passwords. In contrast, 23 (or almost half) of the respondents not using access control were reporting from organizations with less than $100 million in revenues.

Apparently those not using access controls have made their security decisions with appropriate insight: they are not among the respondents who report financial losses at the higher end of the spectrum. Indeed, none of these 48 respondents reports a financially significant loss of proprietary information.

Among the past year's "buzzword" technologies, intrusion detection systems (IDSs) were widely deployed (73 percent) and biometrics were not (11 percent). Not surprisingly, though, the organizations that deployed biometrics were more likely than the average organization in the sample to deploy other leading-edge technologies. Some 83 percent of organizations using biometrics said they used encrypted logins; 72 percent used digital IDs or certificates; and 87 percent said they used file encryption. These figures compare to overall averages of 58 percent using encrypted logins, 49 percent using digital IDs or certificates, and 69 percent using file encryption.

Internet Connection is Increasingly Cited as a Frequent Point of Attack



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 445 Respondents/84%
2002: 481 Respondents/96%
2001: 384 Respondents/72%
2000: 443 Respondents/68%
1999: 324 Respondents/62%

That last statistic—that 69 percent of respondents using file encryption—may indicate a mild upward trend. This is up from 58 percent last year, which would be a statistically significant uptick. The five-year average for this question is 59 percent, which lends credence to the notion that the use of encrypted files is increasing.

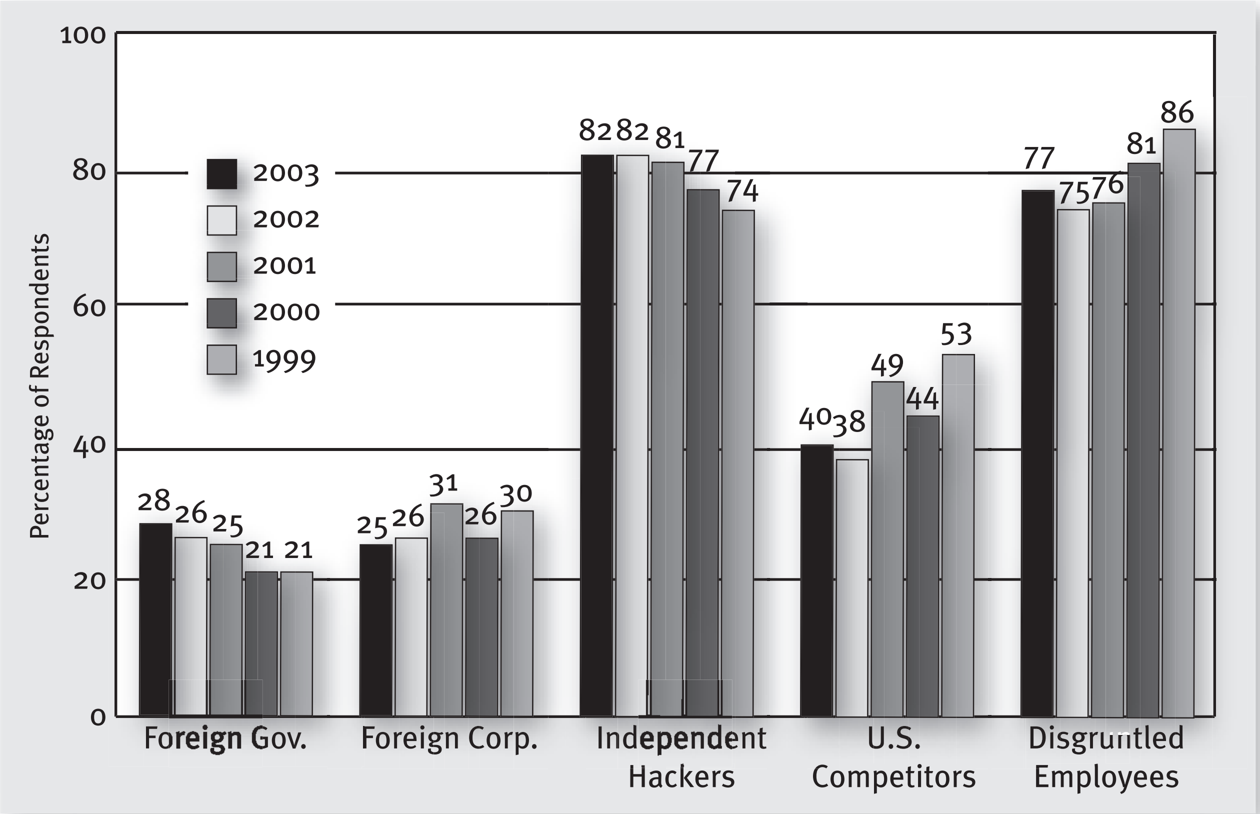
Regardless of the tools used, it is still the case that many respondents simply do not know what's going on within their networks. Fifteen percent of respondents say they don't know whether there was any unauthorized use of their computer systems last year. This is disturbing, one could argue. At the same time, however, it's about the same percentage as always: the average for the past seven years of the survey was that 16.3 percent didn't know.

PROPRIETARY INFO

Throughout the survey's history, the theft of proprietary information has been one of the costliest forms of computer crime. Indeed, since 1999 it has consistently topped the rankings of reported financial losses. This shouldn't be surprising in an economy where a great deal of overall productivity hinges on information and highly technical know-how.

Within the world of the Internet, issues surrounding intellectual property were front and center in 2002. The high-profile news items weren't necessarily about the theft of trade se-

Likely Sources of Attack



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

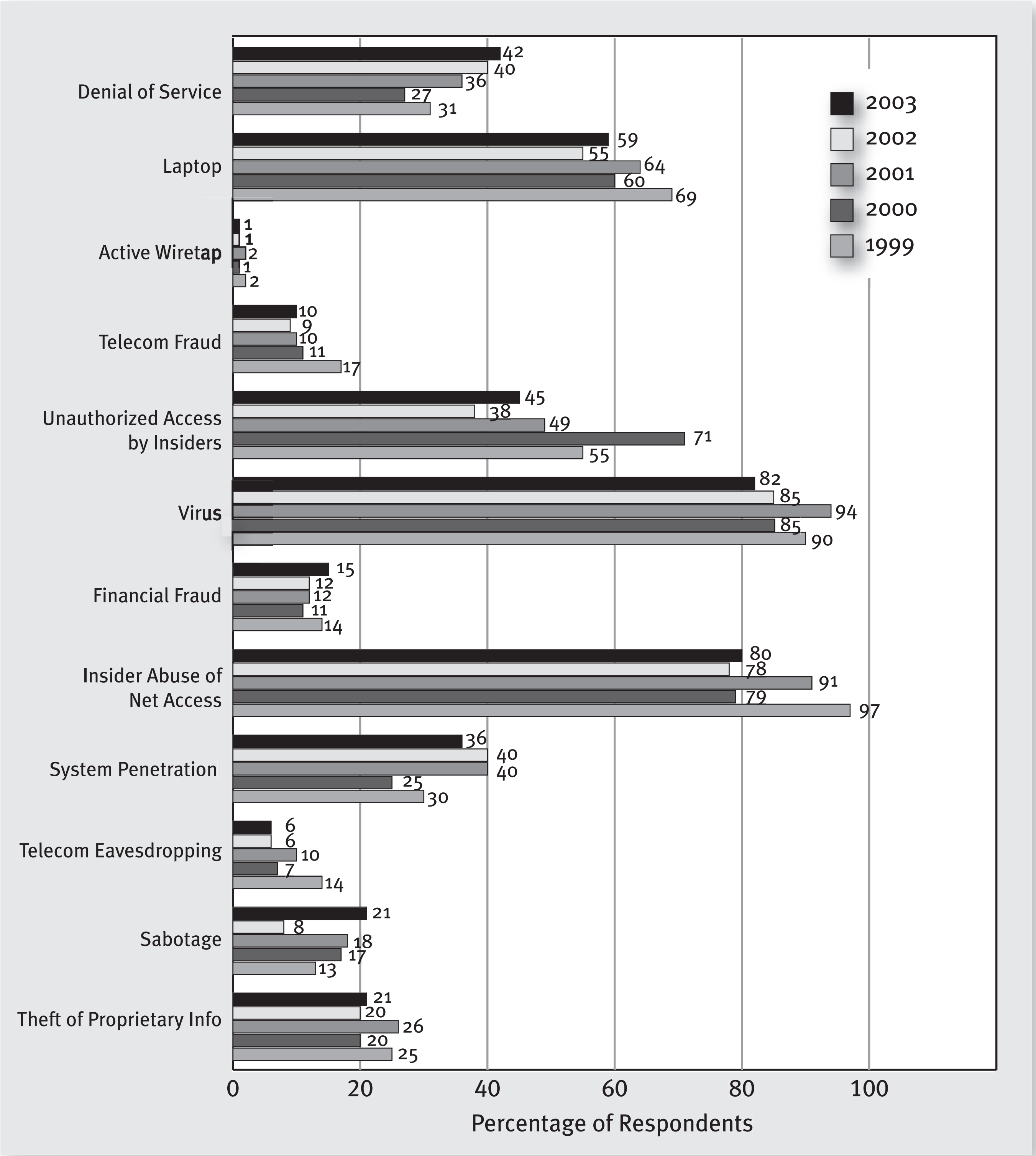
2003: 488 Respondents/92%
2002: 414 Respondents/82%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%

crets, which is the greater threat to most companies, but even focus on copyright infringement has created a climate in which interest in encryption-based controls such as Microsoft's new Digital Rights Management server has increased steadily.

Major intellectual property issues last year included the Supreme Court's consideration of Congress's 1998 extension of the terms of U.S. copyright. What critics termed the "Disney Bill" because it extended (among plenty of other things) that company's control over its Mickey Mouse character, was the eleventh extension to copyright terms in 40 years. The Supreme Court's decision wasn't delivered until January 2003, but the writing was already on the wall in the latter half of 2002: Congress could do what it wanted with copyright terms.

That Congress would want to make terms longer is a clear expression in a general change in corporate and government sensibilities toward more clear and outright ownership of intellectual property. Within this framework, the RIAA in particular was particularly active last year. In April, the organization won a $1 million out-of-court settlement in a suit against Integrated Information Systems (IIS), which had run an internal server where employees traded MP3 files that the RIAA claimed infringed thousands of copyrights. Another settlement with Audiogalaxy.com forced what had been a Napster-like music-trading service into newfound respectability, such that the service now is subscription based and charges users on a per-track basis for

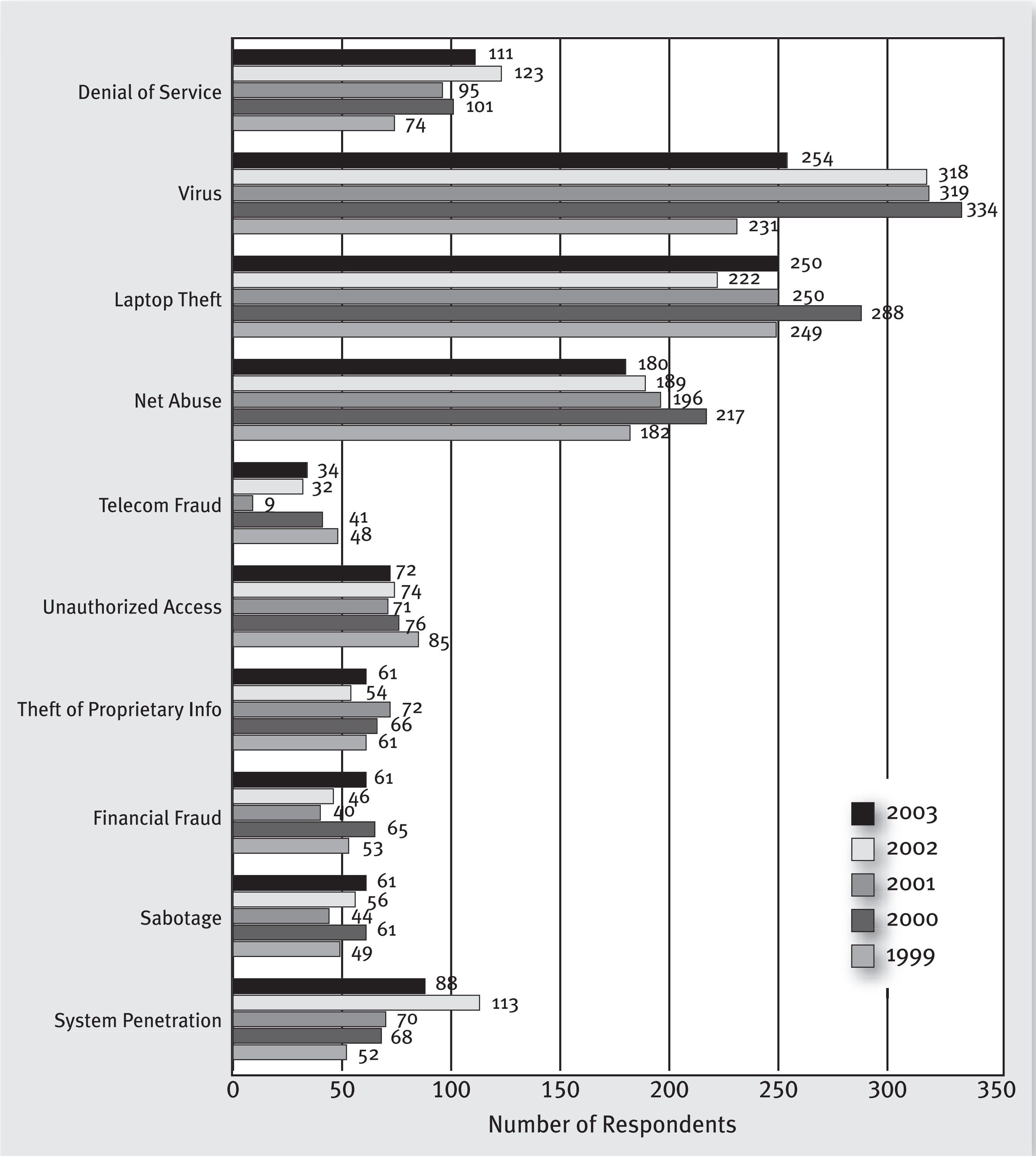
Types of Attack or Misuse Detected in the Last 12 Months (by percent)



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 490 Respondents/92%
2002: 455 Respondents/90%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%

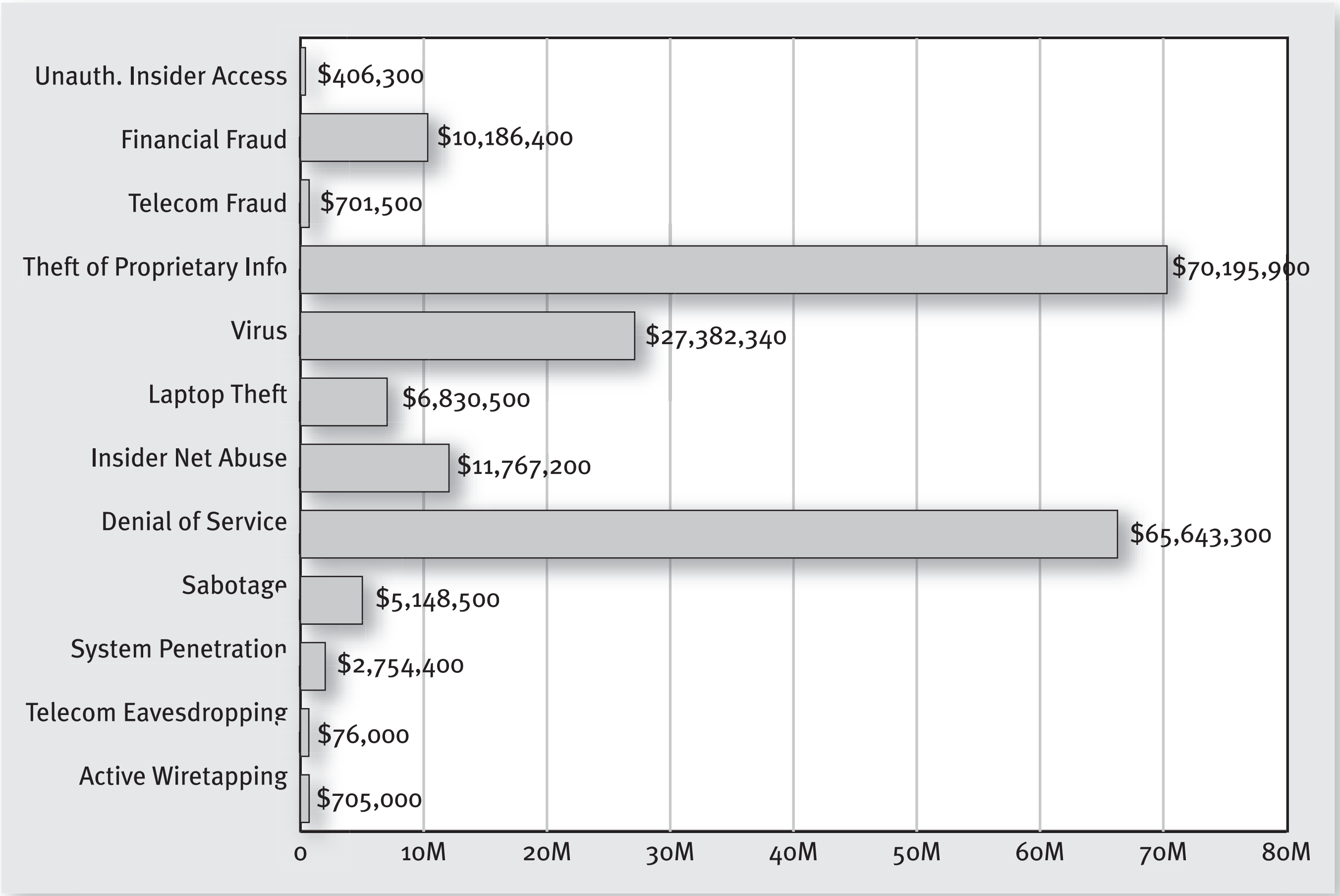
Types of Attack or Misuse in Organizations Reporting Financial Loss (by number)



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 398 Respondents/75%
2002: 404 Respondents/80%
2001: 344 Respondents/64%
2000: 477 Respondents/74%
1999: 376 Respondents/73%

Dollar Amount of Losses by Type



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 251 Respondents/47%

the right to "burn" songs to their own CDs. In September the group obtained a subpoena to obtain subscriber information from Verizon in order to track down the identity of an alleged copyright infringer—an unprecedented move against an individual rather than a company. And although they weren't saying much about it, the RIAA worked rather diligently behind the scenes last year to "poison the well" for music traders, creating and distributing bogus files that appear to be real song files but that in fact contain noise or, in one case in 2003, Madonna cursing out her fans.

This doesn't mean there wasn't plenty of "conventional" theft of business information. Consider the case of Richard Glenn Dopps, who plead guilty to one felony count of "obtaining information from a protected computer." Here's the summary from the Department of Justice's Web page on computer crime cases:

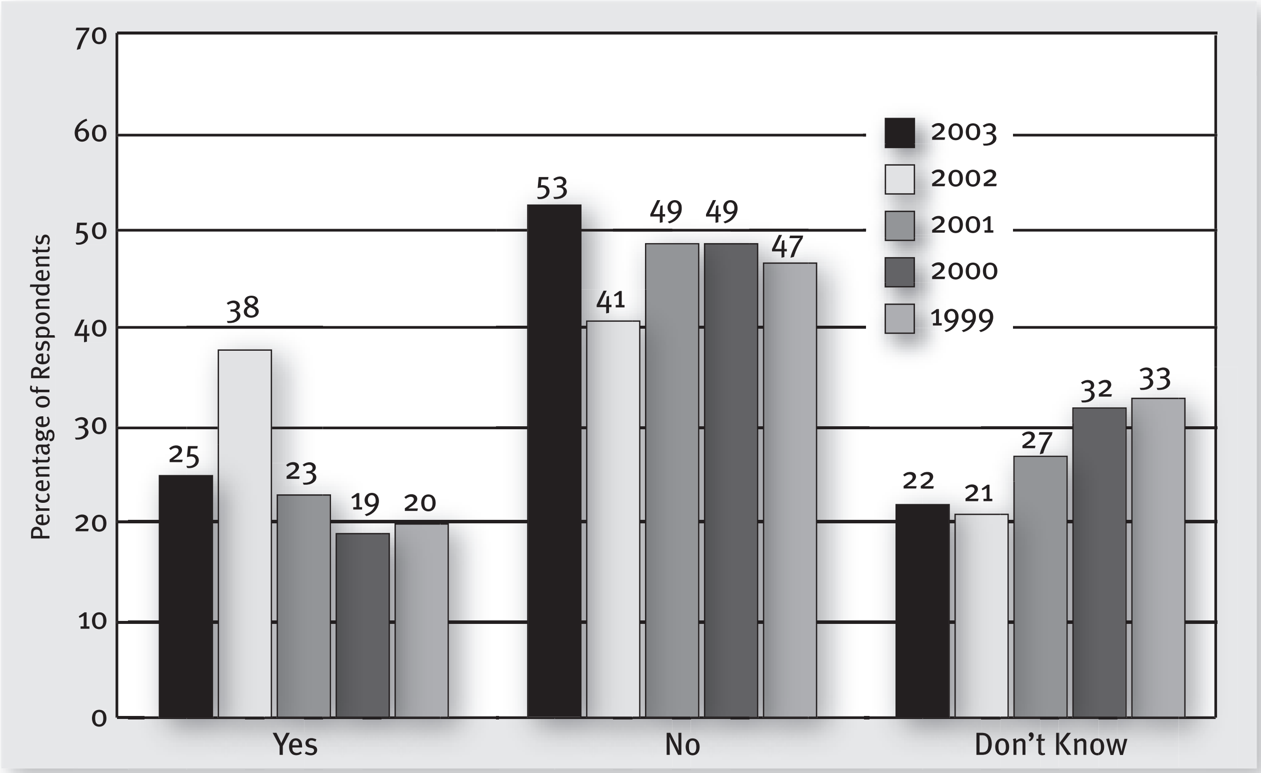
Until February 2001, Dopps was employed by The Bergman Companies (TBC), a contracting firm based in Chino. After leaving TBC to go work for a competitor, Dopps used his Internet connection to gain access to TBC's computer systems on more than 20 occasions.

Once Dopps was inside the TBC systems, he read e-mail messages of TBC executives to stay informed of TBC's ongoing business and to obtain a commercial advantage for his new employer.

Dopps' unauthorized access into TBC's computer system caused approximately $21,636 in damages and costs to TBC.

There are plenty more where this came from. Indeed, browsing through the DOJ's case list (at

Has Your WWW Site Suffered Unauthorized Access or Misuse Within the Last 12 Months?



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 503 Respondents/95%
2002: 472 Respondents/94%
2001: 509 Respondents/95%
2000: 603 Respondents/93%
1999: 479 Respondents/92%

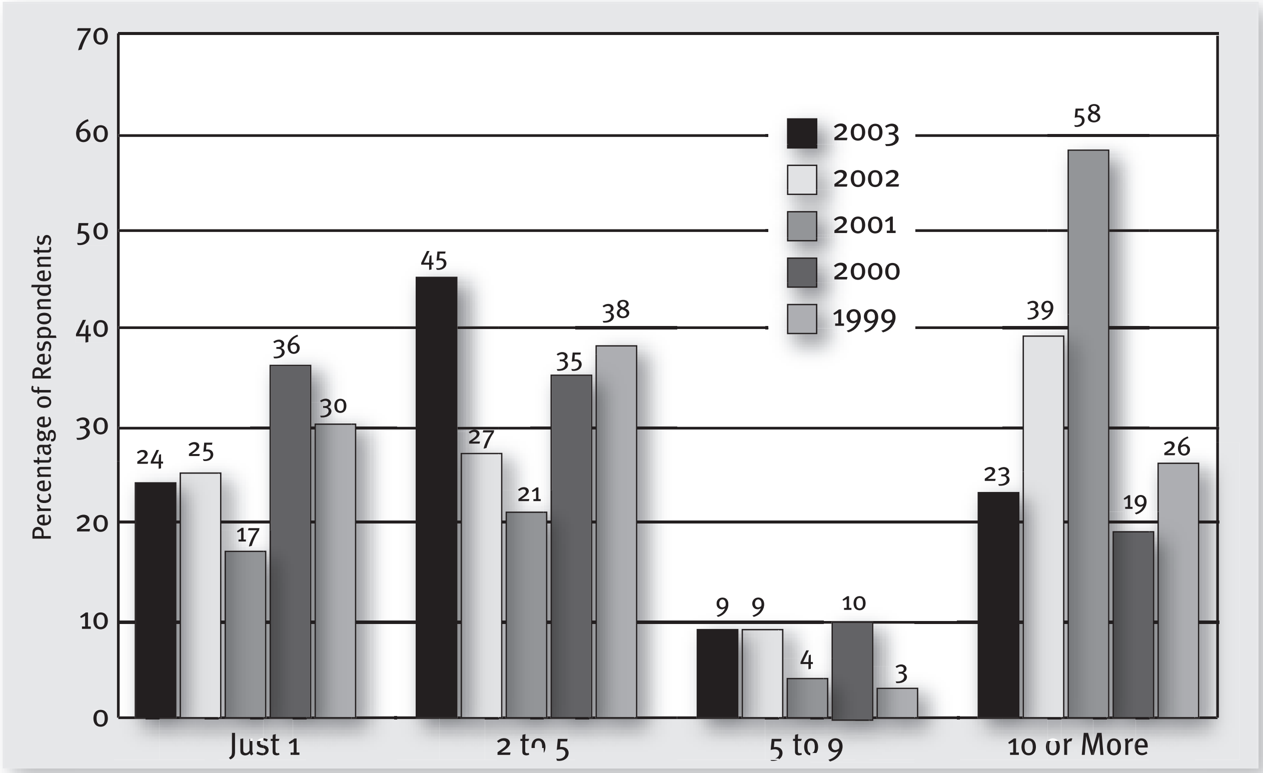
www.usdoj.gov/criminal/cybercrime/cccases.html) is quite instructive, especially if one has any romantic notions about typical convicted cyber criminals being hacker masterminds.

Significant in terms of *solutions* to theft of proprietary data, perhaps, is that the notion of trusted computer platforms made a comeback in 2002. One way of thinking about this general trend is that it focuses on adding security to the end-user desktop computer (though, of course, the same tools will doubtless be adopted on server equipment). At the desktop, there is currently no effective way to tell at a distance (from the perspective of the application server, for example) whether someone or some rogue process has tampered with the software or data running on the desktop.

In 2002, though, chip makers and Microsoft began to tackle this problem both at the hardware and operating system levels. The basic idea is to embed a tamper-resistant security chip into computer systems, providing a location to store information about what the software on the system is supposed to "look" like. Low-level routines in the operating system then use that information to verify the trustworthiness of the system before it is allowed to run software.

This idea of trusted systems isn't new—there was considerable interest in the idea in the 1980s—but it's new to desktop computers. By now, early production of the security chips is well in the works. Already in 2002, IBM had a commercially available notebook computer that incorporated a trusted hardware chip. In early

WWW Site Incidents: If Yes, How Many Incidents?



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 135 Respondents/25%
2002: 244 Respondents/49%
2001: 211 Respondents/40%
2000: 120 Respondents/18%
1999: 92 Respondents/18%
Percentage totals 101% due to rounding

2003, Microsoft began showing prototype variants of its Windows operating system that would natively support this hardware.

Although Microsoft and Intel have both tried to keep the focus of these efforts on the way they protect software from tampering, numerous observers have pointed out that the same mechanisms are exactly what's needed for systems that manage access and use of data—Digital Rights Management systems. Indeed, critics of these trusted computing initiatives argue that what they really do is secure content providers from would-be copyright infringers (and corporations from whistle-blowers, who presumably will no longer be able to send copies of incriminating documents to the press or government agencies), rather than securing users from outside attacks.

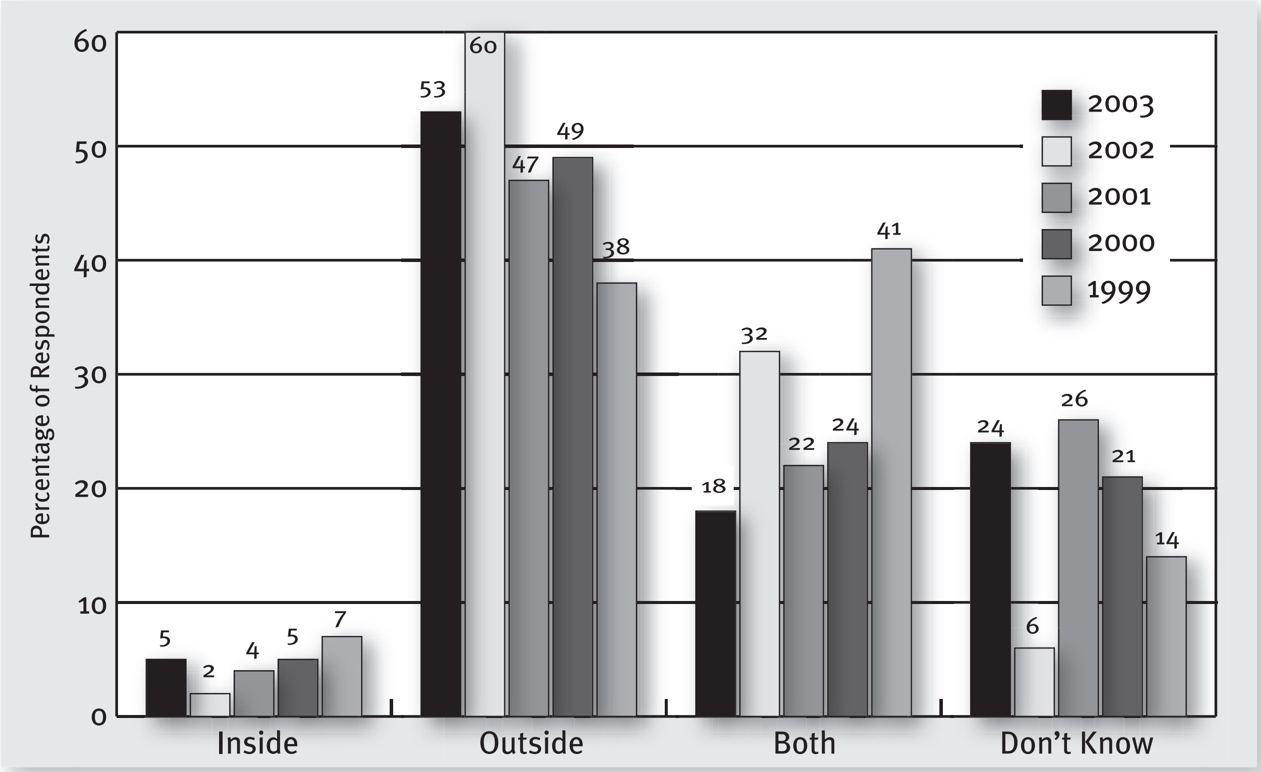
The effects of all this on computer security in the real world, needless to say, will take some time to assess, perhaps as much as five to ten years.

FINANCIAL FRAUD

The survey first asked about losses due to financial fraud in 1997, at which time 12 percent of respondents acknowledged detecting financial fraud. This year's 15 percent reporting financial fraud is the highest level seen in the history of the survey, but is only 1 percent over the previous high, recorded in 1999. So while it's possible that the increase marks the beginning of an upward trend, it seems somewhat more likely that the rate of financial fraud loss has stayed more or less constant, hovering around 13 to 14 percent.

What's really startling about the financial

WWW Site Incidents: Did the Attacks Come From Inside or Outside?



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 181 Respondents/34%
2002: 209 Respondents/42%
2001: 163 Respondents/31%
2000: 153 Respondents/23%
1999: 125 Respondents/24%

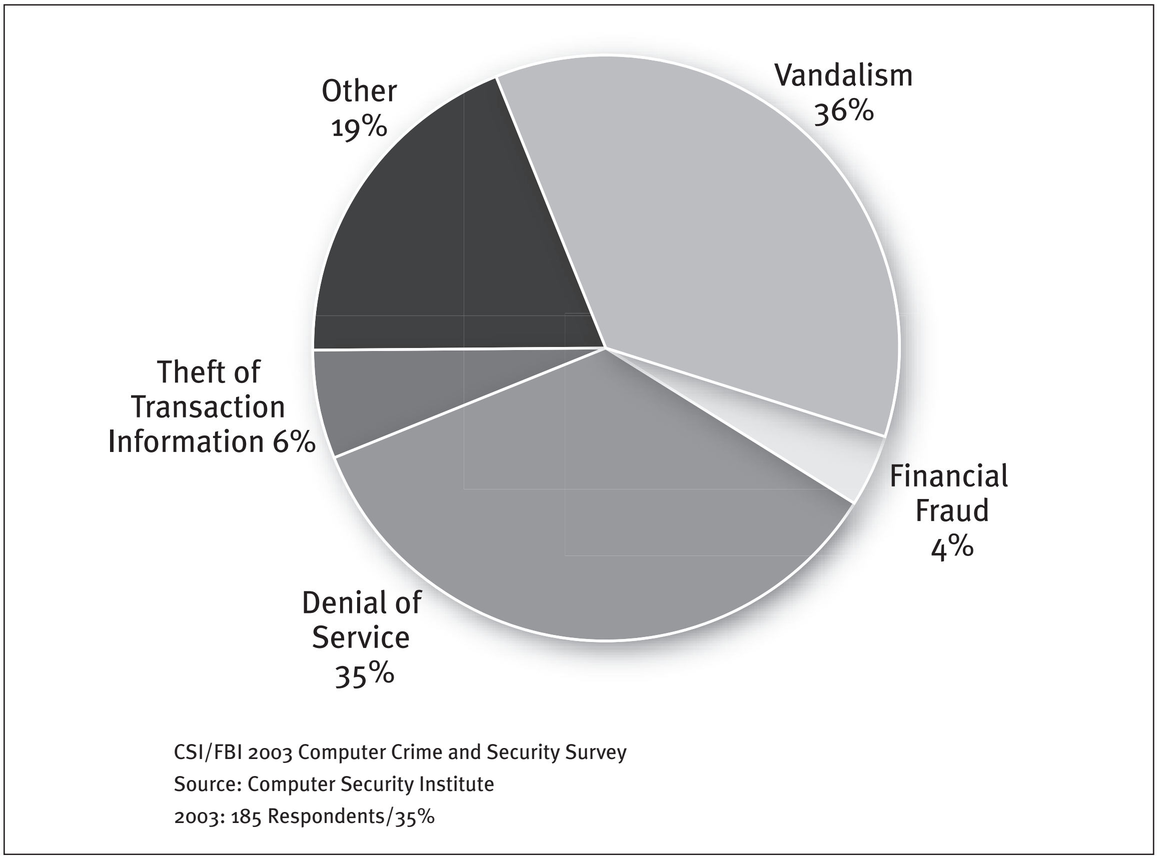
fraud numbers this year, however, are the reported financial losses, which are roughly *one-tenth* what they were last year. It is probably not reasonable to assume anything at all about the broader situation in the U.S. business world, but it may indeed be the case that the sample group in the survey has enjoyed a better-than-average experience in the past year. While 15 percent of respondents reported financial loss—slightly more than in previous years—it is also the case that the most expensive loss reported was $4 million. This is a fraction of last year's highest reported loss, which was $50 million. That single reported instance last year was nearly five times higher than all the losses reported due to financial fraud this year.

As one would expect, the average loss due to financial fraud this year was correspondingly lower than previous years. This year's average of $328,594 was literally millions less than the previous three years, when the averages were $4,632,000 in 2002, $4,420,738 in 2001, and $1,646,941 in 2000.

WHERE TO FIND EXPERTISE

One of the ongoing debates in the information security industry concerns the efficacy of hiring hackers who claim to have reformed. 2002 was an interesting year in this respect because it saw the return to active (but legal) duty of one of society's more widely known hackers, Kevin Mitnick. After a 1995 arrest and conviction on several counts of computer crime the following year, Mitnick was released from prison in 2000. Various restrictions in the terms of his release kept him laying low for a while, but in 2002 he published a book on social engineering, *The Art of Deception*, and launched a

WWW Site Incidents: What Types of Unauthorized Access or Misuse?



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute
2003: 185 Respondents/35%

consulting company, Defensive Thinking. The thinking among most of the survey respondents, though, seems to be that the best defense is steering clear of reformed hackers.

The reasoning among security practitioners seems to be that hackers may reform themselves, but there's no compelling reason to rely on that fact, given that there are lots of skilled practitioners who don't have hacker backgrounds. Yes, it may muddy the waters that some hackers are convicted, where many others commit the same crimes uncaught, and thus can present clean credentials. And yes, it may be possible to hire ex-hackers in roles where they aren't handed access to sensitive production systems. But most respondents don't seem inclined to lose sleep over these distinctions.

The survey asks whether respondents would consider hiring a reformed hacker and the answers are emphatic. Respondents have a habit of answering this question with emphatic circling, exclamation points, and notes scrawled in the margin to support their position (this doesn't happen elsewhere on the survey form).

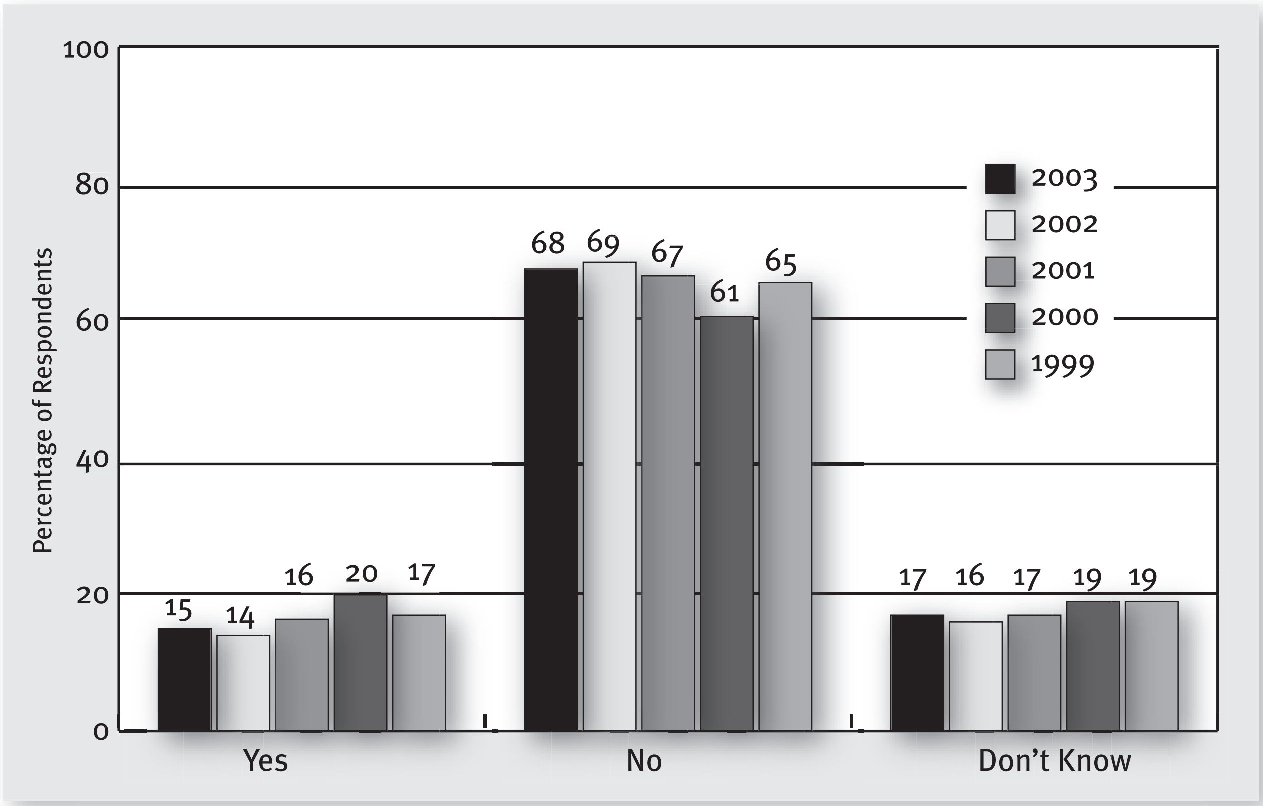
Only 15 percent say they would hire ex-hackers. By contrast, 68 percent say they wouldn't, with 17 percent unsure of their position on the subject.

As a general proposition, though, it would appear that having been caught and successfully prosecuted as a computer criminal is *not* a sure ticket to later success in the security industry, as three-quarters of the marketplace would rather not hire you.

STILL NOT REPORTING

The aim of the annual CSI/FBI Computer Crime and Security survey is not only to gather data on the dark side of cyberspace, but to foster greater cooperation between law enforcement and the private sector so that there is a viable deterrent to cyber crime.

Would Your Organization Consider Hiring Reformed Hackers as Consultants?



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 513 Respondents/97%
2002: 442 Respondents/88%
2001: 524 Respondents/98%
2000: 620 Respondents/96%
1999: 506 Respondents/97%

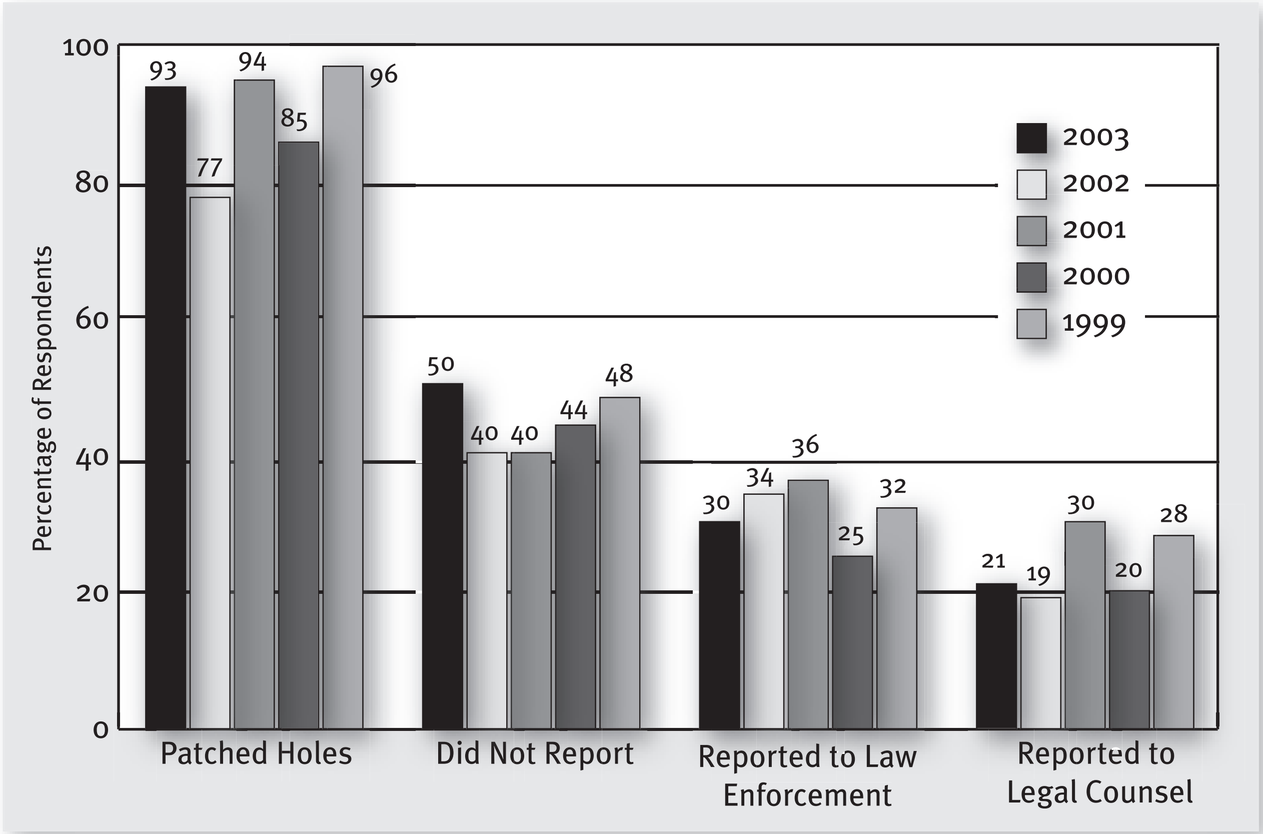
For the first three years of the survey, only 17 percent of those who suffered serious attacks reported them to law enforcement.

In subsequent years, that number roughly doubled. The current year's numbers remain at roughly this doubled level, with 30 percent saying they reported their incidents to law enforcement.

Why isn't this number larger? Only 45 percent of overall survey respondents answered a question about why they didn't report incidents to law enforcement, but of those, fully 53 percent said they were not aware that they *could* report these incidents. While this may seem strange, given that plenty of hacking cases get high-profile media coverage (and the authorities are obviously very much involved in them), it makes more sense in that it isn't always obvious who to turn to when someone has been hacking, say, your Web storefront's customer database. Should you turn to the local police? By and large, you won't get much help there. Should you turn to the FBI? In some cases they can help you and in others they can't (but it sure doesn't hurt to call).

An interesting story that made the rounds early in 2002 makes clear the difficulties that sometimes arise when dealing with cyber crime. Jason Eric Smith sold his Apple Powerbook via eBay, delivering it c.o.d. and receiving what turned out to be a forged bank cashiers check. Now, admittedly, this isn't a case of corporate high-tech hacking and it isn't even directly a case of theft over the wire. On the other hand, it's a straightforward online fraud case where a crime was clearly commit-

If Your Organization Has Experienced Computer Intrusion(s) Within the Last 12 Months, Which of the Following Actions Did You Take?



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 376 Respondents/71%
2002: 389 Respondents/77%
2001: 345 Respondents/64%
2000: 407 Respondents/63%
1999: 295 Respondents/57%

ted—the check was forged. Even when Smith went to the trouble of tracking down the forger himself, though, he couldn't get authorities to break on work from larger cases to drive out and make the arrest. The theft was below the FBI's $5,000 threshold and similarly not a sufficiently significant counterfeiting case for the Secret Service to pursue. Eventually, though, Smith got his man by working with a local police department. Says Smith in a write-up of his pursuit (at www.remodern.com/caught.html):

After talking to two detectives in Chicago, an FBI field agent, an agent in the New Orleans field office of the Secret Service, an agent with the L.A. Secret Service, and having a conference call with a large group of agents from the Chicago Secret Service, I finally was getting somewhere.

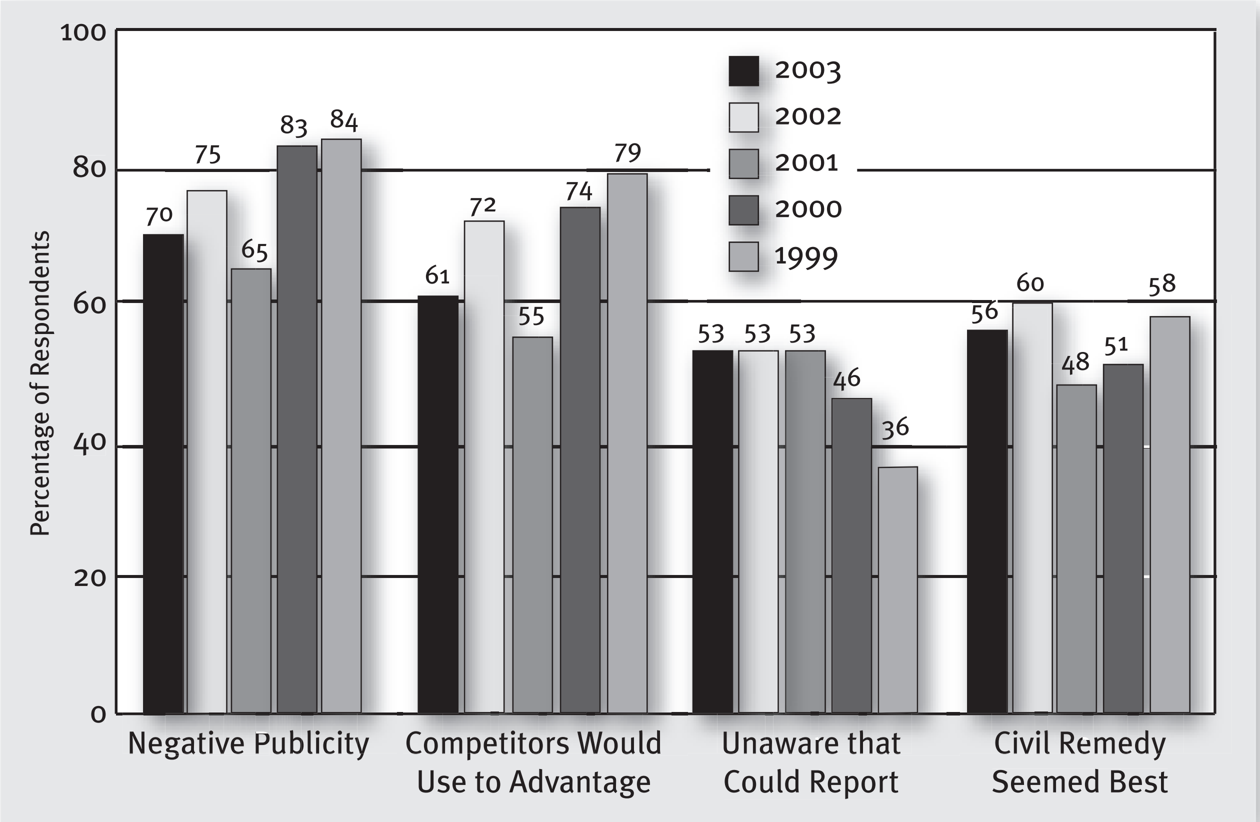
ABOUT THE SURVEY

The CSI/FBI Computer Crime and Security Survey has historically been a fairly informal undertaking, and this year is no exception. Its aim is to heighten security awareness, promote information protection, and encourage cooperation between law enforcement and the private sector.

Informality notwithstanding, there are reasons to have a fair degree of confidence in the statistical rigor of the survey's findings. First, the same survey has been administered for eight straight years and the results this year are certainly quite plausible when compared to averages and trendlines from previous years.

A second point has to do with the nature of the sample taken in this survey. It is certainly

The Reasons Organizations Did Not Report Intrusions in Law Enforcement



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 241 Respondents/45%
2002: 143 Respondents/28%
2001: 151 Respondents/28%
2000: 209 Respondents/32%
1999: 107 Respondents/20%

true that survey recipients are not randomly chosen. They come from a group of security professionals and, among that wider group, they are self selected.

If we ask what the result of that self-selection may be, however, it seems likely that this doesn't undermine the validity of what's reported. These are people who are paying good attention to the security postures and experiences of their organizations. They're arguably in a better position than most, in other words, to know what incidents they've suffered in the past year. It isn't always obvious when a computer system has been attacked—note as proof of this that 22 percent of respondents don't know whether their Web sites were hacked last year—so it stands to reason that people who are paying close attention might provide better-informed responses than those who are not.

Of course, it is also possible that this group might have reason to overstate their losses, as a way of arming themselves with dire statistics to bring to their bosses when the budgeting season rolls around. While this may have seemed likely in the several years when total financial losses moved inexorably upward, it's harder to support this theory given the significant drop in reported losses in this year's survey. Beyond that, though, the "self-interest" theory (if one can call it that) is built on the notion that respondents are somehow aware of some group capability to fudge the numbers and are acting on that notion. If that

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 48-month period

In 2003, 75% of our survey respondents acknowledged financial losses, but only 47% could quantify the losses.

How Money Was Lost

	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses			
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
Theft of proprietary info.	$1K	$100	$1K	$2K	$25M	$50M	$50M	$35M	$3,032,818	$4,447,900	$6,571,000	$2,699,842	$66,708,000	$151,230,100	$170,827,000	70,195,900
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,350	541,000	214,521	27,148,000	5,183,100	15,134,000	5,148,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,0000	76,000
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	300,00	31,254	22,554,500	6,064,000	4,503,000	406,300
Telecom fraud	1K	500	1K	100	3M	8M	100K	250K	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,00	701,500
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000
Laptop theft	500	1K	1K	2400	1.2M	2M	5M	2M	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
												Total Annual Losses	**265,337,990**	**377,828,700**	**455,848,000**	**201,797,340**

CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

were the case, one would expect to find most respondents reporting losses in most categories (why not push up all the losses, after all?). But this is not how individual answers look—most respondents only report three or four categories of loss. Furthermore, considerably more respondents claim various kinds of attacks than report losses for those attacks. One might expect every attack to have a price if the overall interest was padding the numbers.

Assuming that respondents are honest and the numbers legitimate, there is still the basic problem of surveys—they never are as unassailable as you'd like them to be. This survey, like most others, is at best a series of snapshots of how people in the trenches viewed their situation at a given time.

CSI offers the survey results as a public service. The report is free at the CSI Web site (www.gocsi.com), where a hardcopy edition can also be ordered as a print-on-demand document (this is offered at cost).

The participation of the FBI's San Francisco office has been invaluable. They provided input into the development of the survey and acted as our partners in the effort to encourage response. But we have no contractual or financial relationship with the FBI. It is simply an outreach and education effort on the part of both organizations. CSI funds the project and is solely responsible for the results.

Opinions offered in this study are those of the author and the individuals cited and not necessarily those of the Federal Bureau of Investigation, Computer Security Institute, or any other organization.

CONTACT INFORMATION

For referrals on specific criminal investigations:
Mary Kimura, Special Agent
San Francisco FBI Computer Crime Squad,
22320 Foothill Blvd., Hayward, CA. 94541,
Ph: 510-886-7447
nccs-sf@fbi.gov
For general information, go to www.nipc.gov

For information on the CSI/FBI study:
Robert Richardson, Editorial Director
Computer Security Institute,
Home Office,
Ph: 610-604-4604, Fax: 610-604-4606
rrichardson@cmp.com
For general information, go www.gocsi.com

How CSI Can Help

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

Computer Security Institute (CSI) is the world's premier membership association and education provider serving the information security community, dedicated to advancing the view that information is a critical asset and must be protected. Through conferences, seminars, publications and membership benefits, CSI has helped thousands of security professionals gain the knowledge and skills necessary for success. For 30 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

CSI Conferences:

NetSec 2003

June 23-25, 2003, New Orleans, LA

A balanced perspective of managerial and technical issues makes this the most popular conference devoted to network security.

30th Annual Computer Security Conference & Exhibition

November 3-5, 2003, Washington, DC

The world's largest conference devoted to computer and information security

Training:

Awareness
Policies
Intrusion Prevention
Risk Analysis
Internet Security
Windows 2000

Membership Benefits:

Computer Security *Alert* (8 page monthly newsletter)
Computer Security Journal (quarterly)
Annual Computer Security Products Buyers Guide

FrontLine End User Awareness Newsletter

Working Peer Groups

Visit us online

www.gocsi.com

Not a CSI member? To start receiving the Alert, Computer Security Journal and other Membership benefits, go to www.gocsi.com or call Ron Cylc, Membership Coordinator at 215-396-4004.

CSI
COMPUTER
SECURITY
INSTITUTE