CSI
COMPUTER SECURITY INSTITUTE

COMPUTER SECURITY ISSUES & TRENDS

VOL. VII, NO. 1 SPRING 2001

2001 CSI/FBI Computer Crime and Security Survey

By Richard Power, Editorial Director, CSI

The annual "CSI/FBI Computer Crime and Security Survey" is conducted as a public service by the Computer Security Institute (CSI), with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to help raise the level of security awareness as well as to assist in determining the scope of computer crime in the U.S.

Now in its sixth year, the annual release of the survey results is a major international news story, covered widely in the mainstream print and broadcast media. Furthermore, throughout the year, the survey results are referenced in numerous presentations, articles and papers on the nature and scope of computer crime.

Based on responses from 538 computer security practitioners in U.S. corporations and government agencies, the findings of the "CSI/FBI 2001 Computer Crime and Security Survey" confirm the trends that have emerged over the previous years:

❒ Organizations are under cyber attack from both inside and outside of their electronic perimeters

❒ A wide range of cyber attacks have been detected

❒ Cyber attacks can result in serious financial losses

❒ Defending successfully against such attacks requires more than just the use of information security technologies

Patrice Rapalus, CSI Director, elaborates.

"The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with information security."

Bruce J. Gebhardt is in charge of the FBI's Northern California office. Based in San Francisco, his division covers fifteen counties, including the continually expanding Silicon Valley area. Computer crime is one of his biggest challenges.

"The results of this year's survey again demonstrate the seriousness and complexity of computer crime. The dynamic vulnerabilities associated with conducting business on-line remain a law enforcement challenge. In an effort to address this challenge the FBI and private sector have joined forces in an information sharing initiative named 'InfraGard.' For more information about InfraGard, please contact your local FBI office or visit the InfraGard website at www.infragard.net."

The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established the National Infrastructure Protection Center (NIPC) located at FBI headquarters and the Regional Computer Intrusion Squads located in selected offices throughout the United States.

The NIPC, a joint partnership among federal agencies and private industry, is designed to serve as the government's lead mechanism for preventing and responding to cyber attacks on the nation's infrastructures. (These infrastructures include telecommunications, energy, transportation, banking and finance, emergency services and government operations).

The Regional Computer Intrusion Squads investigate violations of Computer Fraud and Abuse Act (Title 8, Section 1030), including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes.

Computer Security Institute is the most prestigious international membership organization specifically serving the information security professional. Established in 1974, CSI has thousands of members worldwide and provides a wide variety of information and education programs to assist practitioners in protecting the information assets of corporations and governmental organizations.

Briefing Notes

Who We Asked

Most respondents work for large corporations. The heaviest concentrations of respondents are in the high-tech (21%) and financial services (17%) sectors. Manufacturing is the next largest industry segment (10% of respondents).

When taken together, federal (8%) state (6%) and local (1%) government agencies comprise another 15% of respondents.

Organizations in other vital areas of the national infrastructure also responded—for example, medical institutions (7%), telecommunications (4%) and utilities (3%).

The responses come from organizations with large payrolls—for example, 27% reported 10,000 or more employees and 11% reported from 5,001 to 9,999 employees.

Thirty-nine percent of respondents in the commercial sector reported a gross income over $1 billion, 9% reported gross income of from $501 million to $1 billion, and 17% reported gross income of from $100 million to $500 million. Don't be dissuaded by the fact that only 538 organizations are represented in this survey. Consider the numbers of employees at work in those organizations. Consider the gross income of the private sector enterprises. Consider the industry segments represented. Consider the impact of large-scale lay-offs at major corporations during the economic downturn of 1Q01.

Indeed, the results of the annual CSI/FBI survey offer a unique glimpse at some of the vulnerable underpinnings of power and prosperity in the U.S.

The types of incidents reported (whether illegal, litigious or simply inappropriate), as well as the trends that the six-year life of the survey confirm, have the potential to do serious damage to U.S. economic competitiveness.

Unless information security is the focus of concerted efforts throughout both the public and private sector, the rule of law in cyberspace as well as U.S. leadership in the global marketplace will be undermined.

What They Use

For the fourth year in a row, we asked what kind of security technologies respondents were using. Writing in his insightful (and free) e-mail newsletter, *Cryptogram,* Bruce Schneier of Counterpane Systems (www.counterpane.com), one of the luminaries in the field of information security, sums up the results.

"What's interesting is that all of these attacks occurred despite the wide deployment of security technologies: 95% have firewalls, 61% an IDS, 90% access control of some sort, 42% digital IDs, etc. Clearly the technologies are not working."

Yes. It is compelling. Ninety-five percent use firewalls, 98% use anti-virus software. And yet...

Of course, there are many unanswered questions. For example, how many firewalls do you have and where are they deployed? Where are your anti-virus software programs running and how often are they updated? Etc., etc., etc.

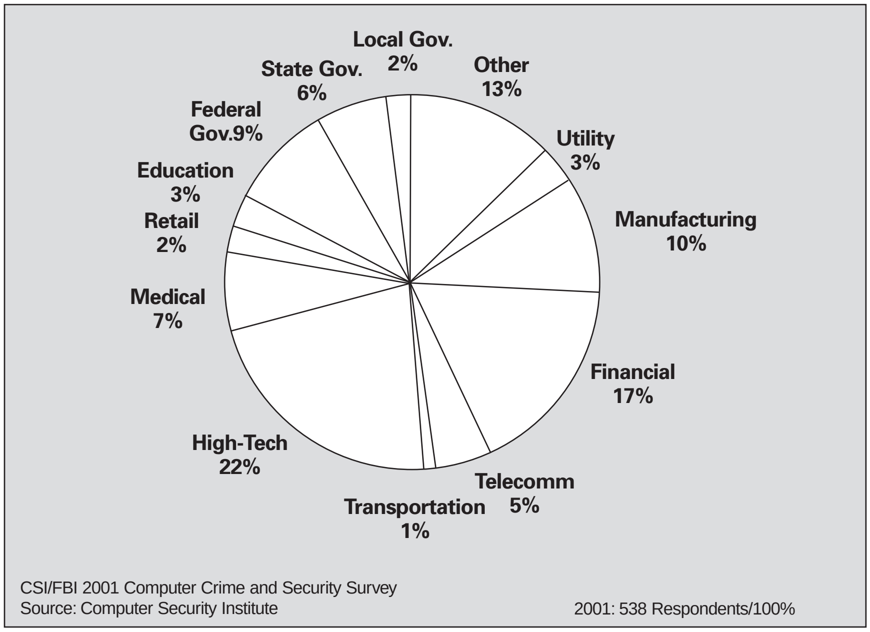
There is no end to the hair-splitting, and yes, digging down deeper into the responses would be fascinating. Nevertheless, additional data would not alter the one over-riding lesson that should be taken away from looking at these results—information security is not as simple as deploying technologies.

Too many organizations have yet to come to grips with vital organizational issues. Where should information security report within the corporate structure? Directly to the CIO or the CFO rather than somewhere down in the bowels of IT? How much money should be dedicated to information security overall? At least from 3% to 5% of the total IT budget?

Rebecca Herold, formerly a senior security analyst with the Principal Financial Group (Des Moines, IA) and now a consultant with Netigy (www.netigy.com), explains.

"Protecting networks and information is such a vital component for the success of a business but too many companies still give these security responsibilities to staff who are not qualified or do not have the appropriate background. Companies need to budget for high quality information and network security staff, place them at levels within the organization where they can have input in strategic planning and pro-

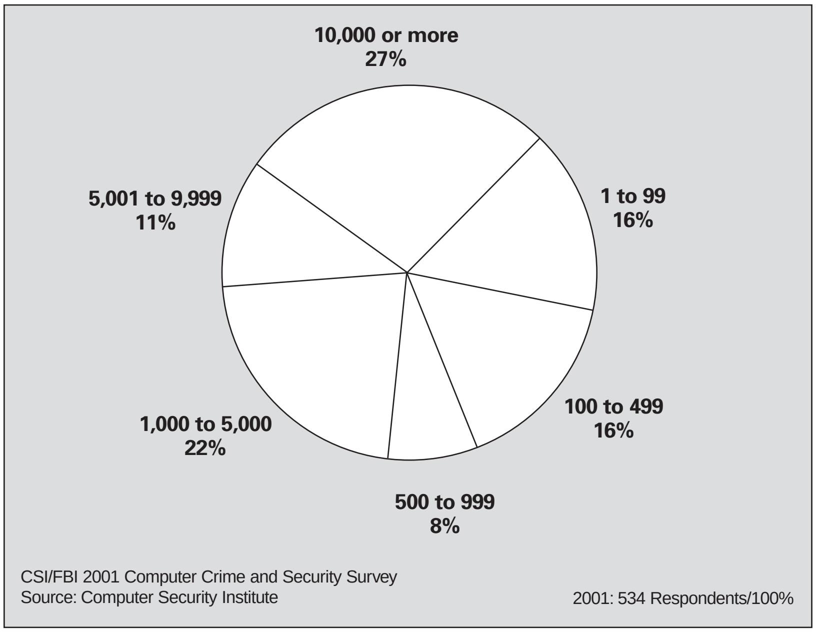
Respondents by Industry Sector



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 538 Respondents/100%

Respondents by Number of Employees



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

vide for effective and efficient security within mission critical applications. The days of placing personnel into positions labeled 'security' that have no influence over security direction and only spend time doing data entry into access control databases at the direction of programmers, secretaries, clerks, and every other position within a company has got to come to an end.

"I still remember being asked in 1995 why I wanted to be in a 'dead-end' job such as security. The person asking me this told me I could only be spending about 4 hours a day working on user IDs and access changes. They told me I should look into doing something with a more promising future, because they didn't think security would even be a position needed to be filled with the 'technical advances' being made. (Oh, this person was an IT manager then, but is now a night-time manager at a convenience store.) It must be accepted that information and computer security is a role that is here to stay, and the importance of which will only increase as our companies become more dependent upon computers and accurate information to stay in business. We must spend some effort helping executive management understand the importance of information security to their organization, and treating their security professionals with the respect and compensation they deserve. Awareness is crucial. We all need to be security educators for our coworkers."

In too many organizations, information security is just one aspect of some overworked network administration staff's responsibilities. It just isn't enough. Indeed, some organizations should considering contracting with professionals who can monitor their networks 24x7 and understand what they are seeing.

But as the ancient Tibetan Buddhist proverb says, "As a thing is viewed, so it appears." Or, as it is re-phrased in the Zen tradition, "Is the glass half-empty or half-full?"

Perhaps there is some good news.

There was a significant increase in those reporting the use of intrusion detection systems (IDS) from 50% in 2000 to 61% in 2001.

In fact, the number of respondents using IDS has increased every year from 35% in '98 to 42% in '99 to 50% in '00 to 61% in '01.

Meanwhile...

The number of respondents who detected system penetration from the outside also rose overall from 23% in '98 to 40% in '01. And the number who cited their Internet connection as a frequent point of attack has increased steadily from 47% in '98 to 70% in '01.

Perhaps the deployment of IDS has helped get a handle on what is really going on?

Another bit of good news from the 2001 survey results is the decline in the number of respondents citing the use of the reusable passwords as a security control from 61% in '99 to 54% '00 to 48% in '01.

Rebecca Herold concurs.

"It's good to see a trend in a decrease of reusable passwords. Getting end-users to use hard- or soft-tokens with their single-use passwords has historically been quite a challenge. Once end-users have experience using them, however, they typically like (or at least accept) the way they work."

Way back in 1995, I transcribed a presentation on problems surrounding the authentication of users delivered by William Hugh Murray of Deloitte and Touche LLP, one of the giants in the field, at CSI's annual conference that year and ran the piece on the cover of the *Computer Security Alert* (No. #147, June 1995).

In the course of his presentation, Murray pronounced the reusable password dead. He gave it a proper eulogy ("it served us well") and consigned it to oblivion ("but its usefulness is at an end").

Murray is an eminently practical man. He knew back then that passwords wouldn't be going away. He just wanted people to know that they should have gone away.

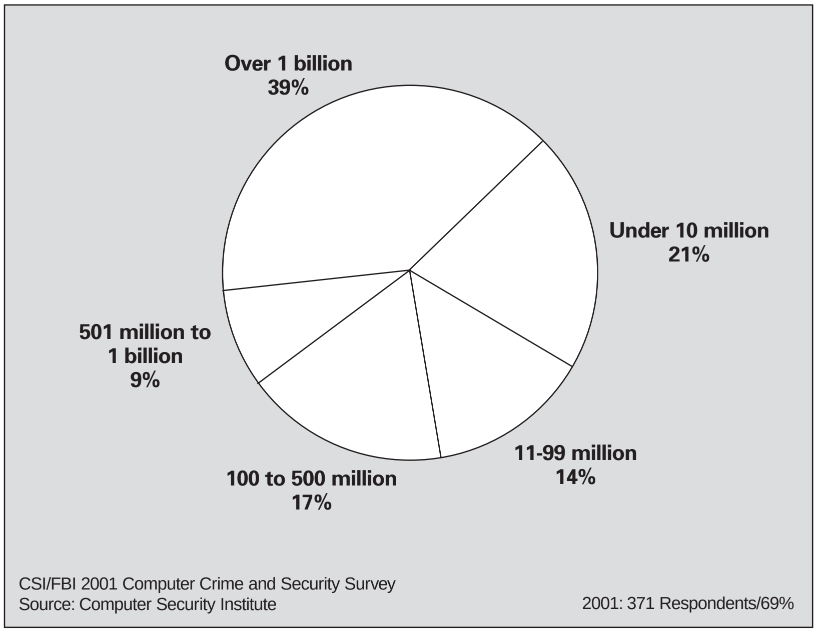
Unfortunately, the harsh reality is that most information security practitioners still toil in environments in which their struggles involve questions like, "How long a period of time should users be allowed before they have to change their passwords? Thirty days? Sixty days? Ninety days?" Incredible.

Of course, Murray was, as usual, way ahead of the curve.

The trends continue

Highlights of the "2001 Computer Crime and Security Survey" include the following:

Respondents by Gross Income



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute
2001: 371 Respondents/69%

- Ninety-one percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Sixty-four percent acknowledged financial losses due to computer breaches.
- Thirty-five percent (186 respondents) were willing and/or able to quantify their financial losses.
- These 186 respondents reported $377,828,700 in losses. (In contrast, the losses from 249 respondents in 2000 totaled only $265,589,940. The average annual total over the three years prior to 2000 was $120,240,180.)

As in previous years, the most serious financial losses occurred through theft of proprietary information (34 respondents reported $151,230,100) and financial fraud (21 respondents reported $92,935,500).

For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%).

Indeed, the rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001.

Thirty-six percent of respondents reported the intrusions to law enforcement; a significant increase from 2000, when only 25% reported them. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

Respondents detected a wide range of attacks and abuses.

Here are some examples of attacks and abuses on the rise:

Forty percent of respondents detected system penetration from the outside (only 25% reported system penetration in 2000).

Thirty-six percent of respondents detected denial of service attacks (only 27% reported denial of service in 2000).

Ninety-one percent detected employee abuse of Internet access privileges (for example, inappropriate use of e-mail systems). Only 79% detected net abuse in 2000.

Ninety-four percent detected computer viruses (only 85% detected them in 2000).

The World Wide Web still has gaping holes

For the third year in a row, we asked some questions about e-commerce over the Internet.

Ninety-seven percent of respondents have WWW sites.

Forty-seven percent conduct electronic commerce on their sites.

Twenty-three percent suffered unauthorized access or misuse within the last twelve months. Twenty-seven percent said that they didn't know if there had been unauthorized access or misuse.

Twenty-one percent of those acknowledging attacks reported from two to five incidents.

Fifty-eight percent reported ten or more incidents.

Ninety percent of those attacked reported vandalism.

Seventy-eight percent reported denial of service.

Thirteen percent reported theft of transaction information.

Eight percent reported financial fraud.

Rik Farrow (www.spirit.com), who teaches CSI's popular course on "Intrusion Attacks and Countermeasures," comments.

"I was amazed to see that 58 respondents had 10 or more Web server incidents. These results left me wondering if the respondents were unable to patch their servers correctly, or were using a particularly insecure product that lead to repeated, successful incidents.

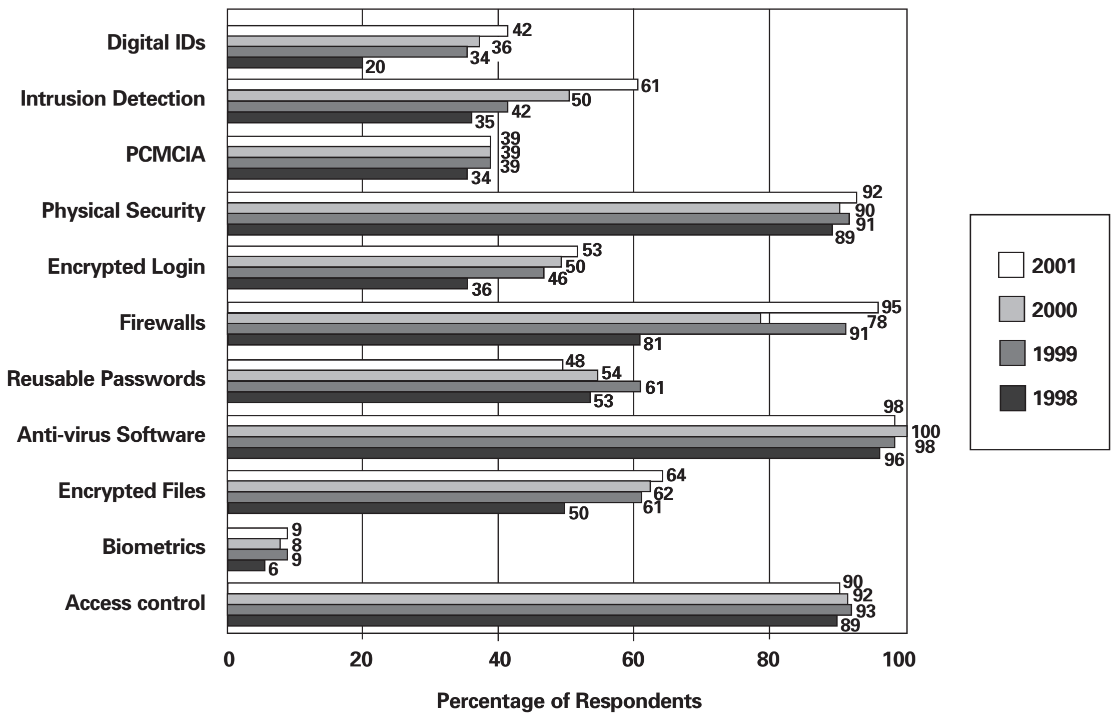
"The number of respondents who 'Don't know' whether an attack came from inside or outside continues to increase. This is also a sad state of affairs.

"It is not enough to secure a server, the server must be monitored for changes or unexpected network traffic that can indicate a subtle, unanticipated, attack. All successful attacks are 'unanticipated' really, aren't they? Or the organization would have taken steps to prevent the attack, or at least be notified if they expected such a thing might occur."

The threat to e-business is real

On MSNBC's recent "Silicon Valley Summit II," a group of high-profile "technology leaders," including Yahoo! founder Jerry Yang, Amazon founder Jeff Bezos and Microsoft CEO Steve Ballmer, sat on high chairs in front of a live audience. With the cameras rolling, Yang, Bezos, Ballmer and a few of the other high lords of the Internet economy engaged in a freewheeling conversation with network TV news anchor Tom Brokaw. They did their best to put a positive spin on the precipitous crash in the value of dot.com stocks, which drove the NYSE and NASDAQ down the tubes. They also

Security Technologies Used



CSI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 530 Respondents/99%
2000: 629 Respondents/97%
1999: 501 Respondents/96%
1998: 512 Respondents/98%

touched on some other timely issues, for example, Napster and the "Digital Divide." They even paid some lip service to the problem of "privacy on-line." But neither Brokaw nor his guests dared draw too much attention to the underbelly of doing business in cyberspace.

Three stories that broke in the days before and after MSNBC's Internet CEO love-fest deliver all the evidence you need to know what's coming.

Three days before MSNBC's confab of dot.com tycoons, the National Infrastructure Protection Center (NIPC), a cyber crime and terror crisis center run by the FBI, released a bulletin informing the public that more than forty targeted companies located in twenty states had been identified and notified of ongoing investigations by fourteen FBI field offices and seven U.S. Secret Service field offices into a series of organized hacker activities specifically targeting U.S. computer systems associated with e-commerce or e-banking. NIPC also disclosed that the investigations had disclosed several organized hacker groups from Eastern Europe, specifically Russia and the Ukraine, that have penetrated U.S. e-commerce computer systems.

The day after the "Silicon Valley Summit," the results of the sixth annual CSI/FBI survey documenting computer crimes and security breaches at Fortune 500 corporations and large government agencies were released.

Less than a week later, the newspaper headlines were dominated by the announcement of the arrest of Abraham Abdallah, a 32-year-old Brooklyn, NY high-school dropout working as a busboy.

Abdallah, already a convicted swindler, was arrested as he was picking up equipment for making bogus credit cards, but he is suspected of already having stolen millions of dollars. In his possession were the social security numbers, addresses, and birthdates of 217 people whose names appeared in a *Forbes Magazine* list of the 400 richest people in the U.S. Law enforcement officials claim that Abdallah also had over 400 stolen credit-card numbers, and had used computers in his local library to access the Web for information gathering on his victims.

Abraham Abdallah is being held for $1 million bail. His activities were detected after an e-mail request to transfer $10 million from a Merrill Lynch account of one of his targets. The cops found mailboxes he had rented in various names and other evidence. (His defense attorney said Abdallah is innocent, and that prosecutors had "made an unfair leap from possession of this information to an inference that there was an attempt to take money.") However the case against Abdallah is resolved, the mass of evidence illustrates that the dire warnings you read about security and privacy in cyberspace are quite accurate.

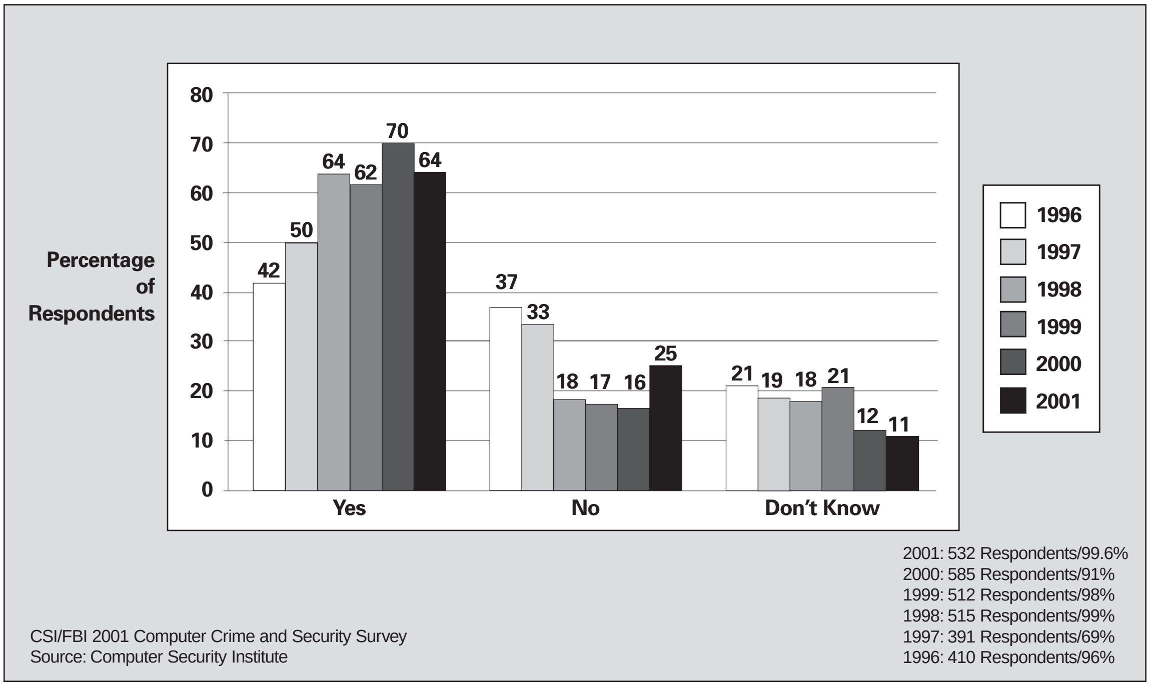
What's the problem? All those bright, bespectacled dot.com multi-millionaires driving around Silicon Valley in SUVs, talking on cell phones, speak with great reassurance about Internet security: "Ah yes, security is very important. Buy this, plug it in here. There now. Everything's secure."

So how does a convicted felon working as a busboy in Brooklyn amass a fortune by co-opting the good name and great credit of over two hundred of the world's most important and influential people?

Well, consider some scenarios. All the suspect would need to log on to Equifax or some other on-line credit history provider and get access to your personal credit records is your social security number. All the suspect would need to buy or sell from your on-line stock portfolio is your user name and password. All the suspect would need to transfer funds from your on-line bank account is your user ID and password.

How easy is it to get such tidbits of information? To paraphrase one of the great love sonnets, "How do I defraud you? Let me count the ways..." Here are some real-world incidents that could have fueled just such a cyber fraud spree.

Unauthorized Use of Computer Systems Within the Last 12 Months



2001: 532 Respondents/99.6%
2000: 585 Respondents/91%
1999: 512 Respondents/98%
1998: 515 Respondents/99%
1997: 391 Respondents/69%
1996: 410 Respondents/96%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Of course, the critical info could simply be hacked.

Here are some examples.

Organizers of an annual meeting of global leaders in the Swiss Alps said it appeared hackers obtained proprietary data (for example, credit card numbers, passport numbers and cell phone numbers) of thousands of prominent people. Reporters for the European newspaper, *Sonntags Zeitung*, were shown data on a CD-ROM containing 80,000 pages of information, including information on U.S. President Bill Clinton, who was the featured speaker at Davos a year ago. *Sonntags Zeitung* also reported that the CD-ROM contained data on 27,000 people, including former U.S. Secretary of State of Madeleine Albright, South African President Thabo Mbeki and top CEOs.

A Swedish hacker stored music and video files on a server at Indiana University (IU) that had apparently been left unprotected after a crash. In the process of their investigation, IU noticed that a file of over 3,100 student names and SSNs had been copied from the server.

A hacker gained access to confidential medical information at the University of Washington Medical Center, using the Internet to download thousands of names, conditions, home addresses and SSNs.

Perhaps some of the e-business sites that you use have experienced problems? Perhaps some of the businesses that you worked for have been targeted?

Recently, a glitch in AT&T's Web site exposed billing and account information for thousands of small businesses. The flaw allowed AT&T small business customers to view other customers' account information. Also, the on-line brokerage house of Charles Schwab Corp. recently confirmed its Web trading site was briefly vulnerable to a security flaw that could allow an intruder to hijack subscribers' accounts.

Amazon.com-based book service Bibliofind.com was the target of a hacker attack that compromised some 98,000 customer records and forced the company off-line for awhile. The hacker downloaded customer records, including names, addresses and credit card numbers.

But hacking isn't the only way a cyber criminal could get hold of the little bit of leaven needed to cook your credit. The critical info could be bought from insiders.

A 12-year veteran of the U.S. Drug Enforcement Administration (DEA) plead not guilty in federal court in Los Angeles to charges of illegally selling sensitive information about private citizens pulled from federal and state law enforcement computers. Special agent Emilio Calatayud is charged in an eleven count indictment with wire fraud, bribery and violation of the Computer Fraud and Abuse Act for allegedly selling 'criminal history and law enforcement information" to private investigations firm Triple Check Investigative Services in Los Angeles.

The critical info could even have been physically stolen.

The details of a break-in at the Gresham, Oregon Department of Motor Vehicles office late last year indicate that the thieves were well prepared. They took less than two minutes to abscond with computer equipment containing personal information on 3,215 people who had recently obtained licenses, plus blank cards and a machine for making bogus drivers' licenses and ID cards.

These are only a few of the ways that the one or two tidbits of information someone would need to commit fraud could be obtained.

Industrial espionage vs. information-age espionage

The conventional wisdom is that industrial espionage is predicated on the turning of the insider. You bribe, blackmail and/or seduce someone who works for your competitor. You get to the trade secrets you want through subterfuge of that sadly compromised human being. But information-age espionage is in some ways cleaner, quicker, more stealthy. You simply hire someone to hack into your competitor's internal networks and steal the secrets you covet in bits and bytes.

Just as information warfare doesn't take the place of blood and

How Many Incidents? How Many From Outside? How Many From Inside?

How Many Incidents?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2001	33%	24%	5%	1%	5%	31%
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29
1998	61	31	6	1	2	n/a
1997	48	23	3*	n/a	n/a	27
1996	46	21	12	n/a	n/a	21

2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%, 1998: 234 Respondents/45%, 1997: 271 Respondents/48%, 1996: 179 Respondents/42%

How Many From the Outside?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2001	41%	14%	3%	1%	3%	39%
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39
1998	74	18	6	0	3	xx
1997	43	10	1*	n/a	n/a	45
1996	n/a	n/a	n/a**	n/a	n/a	n/a

2001: 316 Respondents/59%, 2000: 341 Respondents/53%, 1999: 280 Respondents/54%, 1998: 142 Respondents/27%, 1997: 212Respondents/41%, 1996: n/a

How Many From the Inside?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2001	40%	12%	3%	0%	4%	41%
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35
1998	70	20	9	1	1	n/a
1997	47	14	3*	n/a	n/a	35
1996	n/a	n/a	n/a**	n/a	n/a	n/a

2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%, 1998: 234 Respondents/45%, 1997: 271 Respondents/48%, 1996: 179 Respondents/42%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

* Note: In '96 and '97, we asked only "11 or more."
** Note: In '96, we didn't ask this question.

guts industrial age warfare, information-age espionage doesn't take the place of turning of insiders–but it does mean that you have something else to worry about.

Rik Farrow comments.

"I believe competitors, or organizations working for them, are a much greater source of risk than your respondents realize. It is unlikely that the $151 million loss of proprietary information is all due to independent hackers, or even disgruntled employees. Such losses are due to targeted attacks on the victims by someone with strong, financial motivation to succeed."

Consider some real-world cases.

The U.S. Navy's Criminal Investigative Service (NCIS) is in the throes of an investigation into how and why an as yet unidentified hacker stole the source code to OS/Comet from a computer at the U.S. Navy's naval research lab in Washington, D.C.. in an attack conducted on Christmas Eve, 2000. OS/Comet was developed by Exigent International (Melbourne, FL), a U.S. government contractor.

The software has been deployed by the U.S. Air Force on the NAVSTAR Global Positioning System (GPS) from its Colorado Springs Monitor Station, which is part of the U.S. Space Command.

A copy of the OS/Comet source code was found during a police swoop in Sweden on a computer company whose identity has not been revealed.

The intrusion appears to have emanated from a computer at the University of Kaiserslauten in Germany, which was used to download the software's source code via the Web and the service provider Freebox.com, which is owned by the Swedish firm Carbonide.

The hacker known only as "Leeif" was able to hide his or her true identity by breaking into the account of a legitimate Freebox.com user and then using that person's account to distribute the source code to others.

Exigent has filed suit against both Carbonide and the University of Kaiserlautern in Germany. The NCIS's inquiry is being headed by the NCIS headquarters for European affairs in Naples and by its London bureau, which deals specifically with Scandinavia.

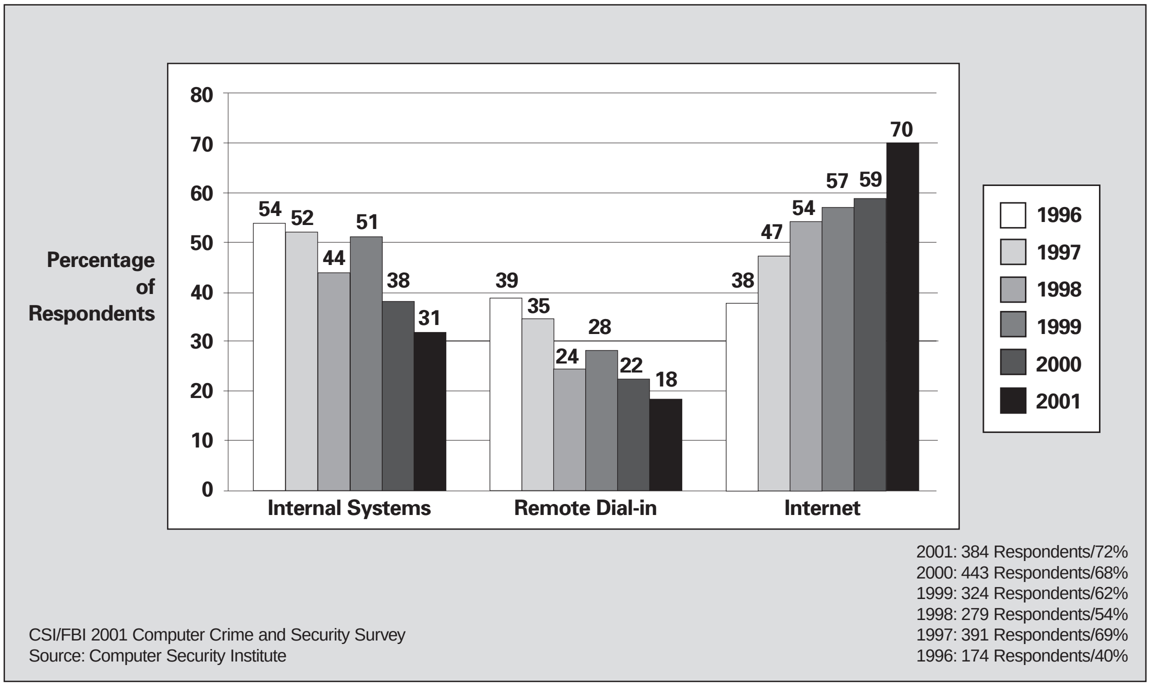
Whether or not "Leeif" is caught, whether or not the act was motivated by some corporation or government's desire to get a hold of and analyze this source code, the incident underscores both the immediacy and potential threat. Even if "Leeif" turns out to be some precocious kid who just wanted to demonstrate his skill and daring—the point is that it happened and it could have happened for the worst of motives as easily as for the least menacing of motives. Indeed, the worst of motives (corporate trade secret theft or intelligence service activity) and the least menacing of motives (an adolescent feeling his digital testosterone kicking in) are not mutually exclusive–the least menacing motive could have provided downstream opportunities for the worst of motives.

Consider an incident involving a high-profile private sector target.

On Friday, October 27, 2000, the news wires caught fire with reports that Microsoft had been hacked and its source code had been compromised. According to Reuters, Microsoft characterized the incident as "a deplorable act of corporate espionage." Reuters quoted Microsoft's Steve Ballmer directly: "It is clear that hackers did see some of our source code."

By the end of the day, I had done interviews with the *Los Angeles Times,* the *Washington Post,* the *New York Daily News,* the *San Jose Mercury News, USA Today, Newsweek,* the BBC, the Associated Press, Reuters and others. These follow-up stories hit the newsstands over the weekend.

Internet Connection is Increasingly Cited as a Frequent Point of Attack



2001: 384 Respondents/72%
2000: 443 Respondents/68%
1999: 324 Respondents/62%
1998: 279 Respondents/54%
1997: 391 Respondents/69%
1996: 174 Respondents/40%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

There are some lessons to be learned from this case.

Indeed, for several years now, it has been obvious to some of us that industrial age espionage was rapidly giving way to information age espionage. Whether or not, if and when, the actual motives of the perpetrator(s) are ever known, the Microsoft source code hack underscores the urgent need for those responsible in vital sectors of the economy to take information age espionage more seriously than they have taken it so far.

It is hard to get over the fact that remote access to Microsoft's source code was "secured" with reusable passwords. Of course, any organization can be hacked, any organization can suffer from a breakdown in their information security. But certainly Microsoft's customers, partners and stockholders should expect something more than reusable passwords to control remote access to source code.

Microsoft has emphatically denied that any harm was done.

Well, perhaps Microsoft could say with some degree of certainty that the copy of the source code resting on that particular server had not been altered. But was it copied in some way? Was it downloaded from that server? Was it studied for a long time even if it wasn't downloaded? If so, the source code is at risk in numerous ways.

If the source code fell into the hands of the underground, it would be analyzed for vulnerabilities that could be exploited.

If the source code fell into the hands of Microsoft's competitors, it could be analyzed by competitors to more easily mimic product features and/or improve on such features.

If the source code fell into the hands of organized criminals, it could be Trojaned, compiled, shrink-wrapped and sold.

Do you really think that most network intrusions are detected?

Do you think that all the implications and consequences of the intrusions that are detected are really understood?

Do you really think that all the network intrusions that are detected are public knowledge?

Do you really think that if there were negative implications to a particular intrusion that the details would be made public knowledge if it could be avoided?

Corporate and government networks are open to attack one way or another or in any one of several ways.

Whether directly or indirectly, corporate trade secrets and government-funded R&D are accessible via those porous networks.

Trade secrets are the life blood of industry, sensitive research is the life blood of military hegemony.

What will your adversaries do? Will a hungry animal eat if it is left alone with its favorite food? Yes, it will. And they do.

Don't get turned inside out

Conventional wisdom says "80% of computer security problems are due to insiders, 20% are due to outsiders."

There are people who cling to this axiom as if some Galileo had just suggested that the Earth might actually be round.

But for the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the number of those citing their Internet connection as a frequent point of attack has been rising, while the number of those reporting both dial-up remote access and their own internal systems as a frequent point of attack have been declining.

As Georgetown's Dr. Denning comments, other results from this year's survey seem to underscore the trend.

"One interesting trend is the shift of perceived threat from insiders to outsiders. For the first time, more respondents said that independent hackers were more likely to be the source of an attack than disgruntled or dishonest insiders (81% vs 76%). Perhaps the notion that insiders account for 80% of incidents no longer bears any truth whatsoever."

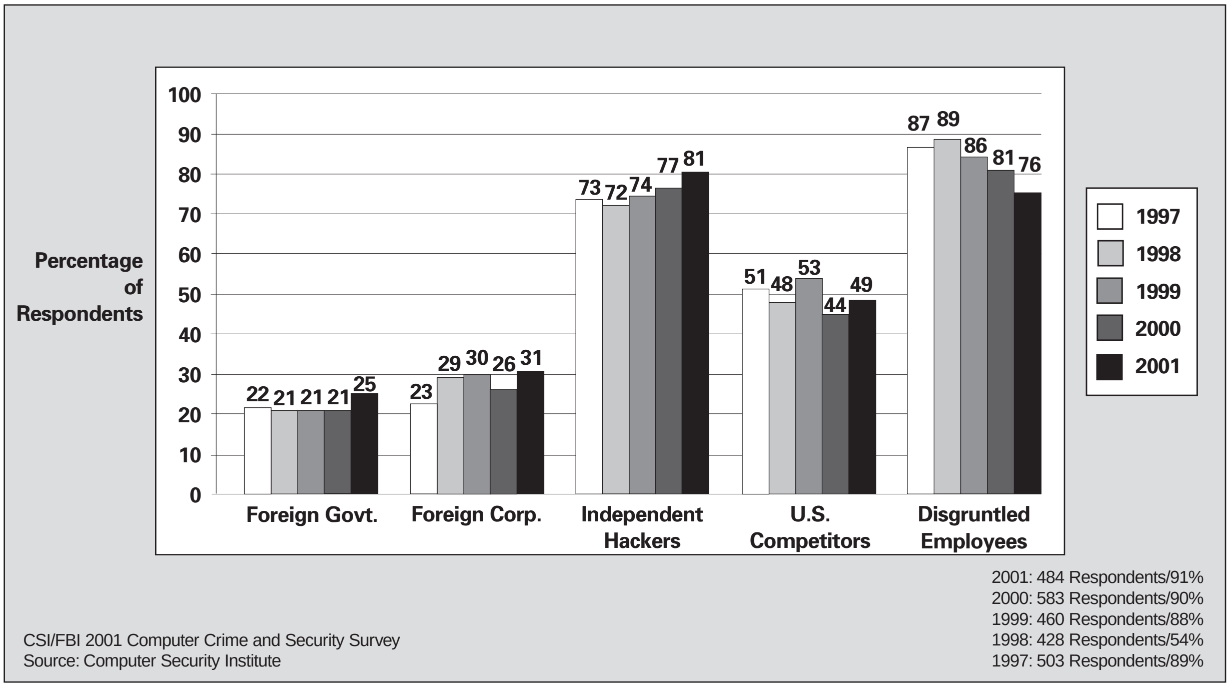
The number of respondents who reported incidents of "unauthorized access by insiders" within the last twelve months also dropped from 71% in 2000 to 49% in 2001.

Clearly, the threat from the outside is increasingly dramatically and has been doing so for several years.

But is the threat from the inside actually decreasing?

It would be premature and dangerous to assume so.

Likely Sources of Attack



2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/54%
1997: 503 Respondents/89%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Consider the case of Robert Hanssen.

On February 21 2001, front page headlines from coast to coast told the story of the FBI's arrest of one of its own counterintelligence agents on charges that he spied for Moscow since 1985.

Incredibly, the 56-year-old Hanssen, described as a "churchgoing father of six" by the *New York Times,* kept his identity concealed not only from the country he is accused of betraying but also to the country to which he is alleged to have sold his soul to for what the *Los Angeles Times* characterized as "cash and diamonds."

On March 5, the *Washington Post* reported that experts were "combing computer systems to try to ensure" that Hanssen, who it referred to as a "highly skilled programmer" did not sabotage them or create "software vulnerabilities" that could be exploited by Russian intelligence.

Did Hanssen have access to Interlink, the highly secured network used by the CIA, the NSA and other elements of the U.S. intelligence community to share information? Officials declined to confirm or deny Hanssen had such access, but if he did, according to the *Post*, "the damage would be deep and difficult to assess."

Certainly, Hanssen was a frequent user of the FBI's internal network, the Automated Case Support System, which "contains classified records of investigations."

The FBI's 108 page affidavit filed in court is an astonishing record of insider espionage activity. It is also a humbling computer security horror story, and as such it should be read by anyone working in the field of information security. In the course of his 15 years, according to the government document, Hanssen is alleged to have stolen dozens of files from the FBI's computer network, and passed on these secrets to his handlers via numerous diskettes.

If someone working within the inner sanctum of U.S. counterintelligence would risk ruin and possibly execution for pay-offs totaling a measly $1.4 million, do you really believe that a disgruntled or dishonest insider with a screw or two loose wouldn't risk far less to betray your corporate secrets?

There were many cases of unauthorized access, sabotage and other security breaches by disgruntled or dishonest insiders.

Joseph Martin Durnal, 22, who broke into his former employer's computer system and sent e-mails–including one that said the company (Peak Technologies) was going out of business–to hundreds of employees received a suspended sentence and was told to pay the company more than $48,000 in restitution.

Investigators identified Durnal, who once worked as a contract employee for the business, through the telephone number used to dial into the network.

Abdelkader Smires, 31, a database engineer angry at his employer, was arrested on charges of using codes to disable computers in a three-day cyber attack on the company, authorities said. Computers at Internet Trading Technologies crashed for several hours over three-day period. The attacks were traced to a computer at Queens College and authorities determined that Smires, who had once taught computer science there, had been using that computer.

Why the drop then in those respondents reporting internal systems as a frequent point of attack? It is quite conceivable that there are more attempted attacks from the outside then the inside within any one organization. There is only a finite number of employees, there is a far bigger world of potential attackers beyond your own internal systems. Yes, it is quite conceivable to me that there are more door knobs rattled from the outside then from the inside. It is also conceivable to me that there has been some decline in attacks from inside in some organizations that take information security seriously and have done the hard work of implementing a comprehensive, enterprise-wide approach. Why? Because of increased monitoring of employee on-line activity as well as increased awareness of the consequences through user education programs.

Yes, more good news. The glass is half-full.

But as the Hanssen case illustrates, the potential damage that one insider can cause could be devastating whether to the future of a single corporation or an entire people.

Consider the insightful comments of Dr. Eugene Schultz in an editorial for *Information Security Bulletin* (Vol. 6, #2, March ‘01).

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 60-month period.

How money was lost

	Respondents w/ Quantified Losses					Lowest Reported					Highest Reported				
	'97	'98	'99	'00	'01	'97	'98	'99	'00	'01	'97	'98	'99	'00	'01
Theft of proprietary info.	21	20	23	22	34	$1K	$300	$1K	$1K	$100	$10M	$25M	$25M	$25M	$50M
Sabotage of data of networks	14	25	27	28	26	$150	$400	$1K	$1K	$100	$1M	$500K	$1M	$15M	$3M
Telecom eavesdropping	8	10	10	15	16	$1K	$1K	$1K	$200	$1K	$100K	$200K	$300K	$500K	$500K
System penetration by outsider	22	19	28	29	42	$200	$500	$1K	$1K	$100	$1.5M	$500K	$500K	$5M	$10M
Insider abuse of Net access	55	67	81	91	98	$100	$500	$1K	$240	$100	$100K	$1M	$3M	$15M	$10M
Financial fraud	26	29	27	34	21	$5K	$1K	$10K	$500	$500	$2M	$2M	$20M	$21M	$40M
Denial of service	n/a	36	28	46	35	n/a	$200	$1K	$1K	$100	n/a	$1M	$1M	$5M	$2M
Spoofing	4	n/a	n/a	n/a	n/a	$1K	n/a	n/a	n/a	n/a	$500K	n/a	n/a	n/a	n/a
Virus	165	143	116	162	186	$100	$50	$1K	$100	$100	$500K	$2M	$1M	$10M	$20M
Unauthorized insider access	22	18	25	20	22	$100	$1K	$1K	$1K	$1K	$1.2M	$50M	$1M	$20M	$5M
Telecom fraud	35	32	29	19	18	$300	$500	$1K	$1K	$500	$12M	$15M	$100K	$3M	$8M
Active wiretapping	n/a	5	1	1	0	n/a	$30K	$20K	$5M	$0	n/a	$100K	$20K	$5M	$0
Laptop theft	165	162	150	174	143	$1K	$1K	$1K	$500	$!K	$1M	$500K	$1M	$1.2M	$2M

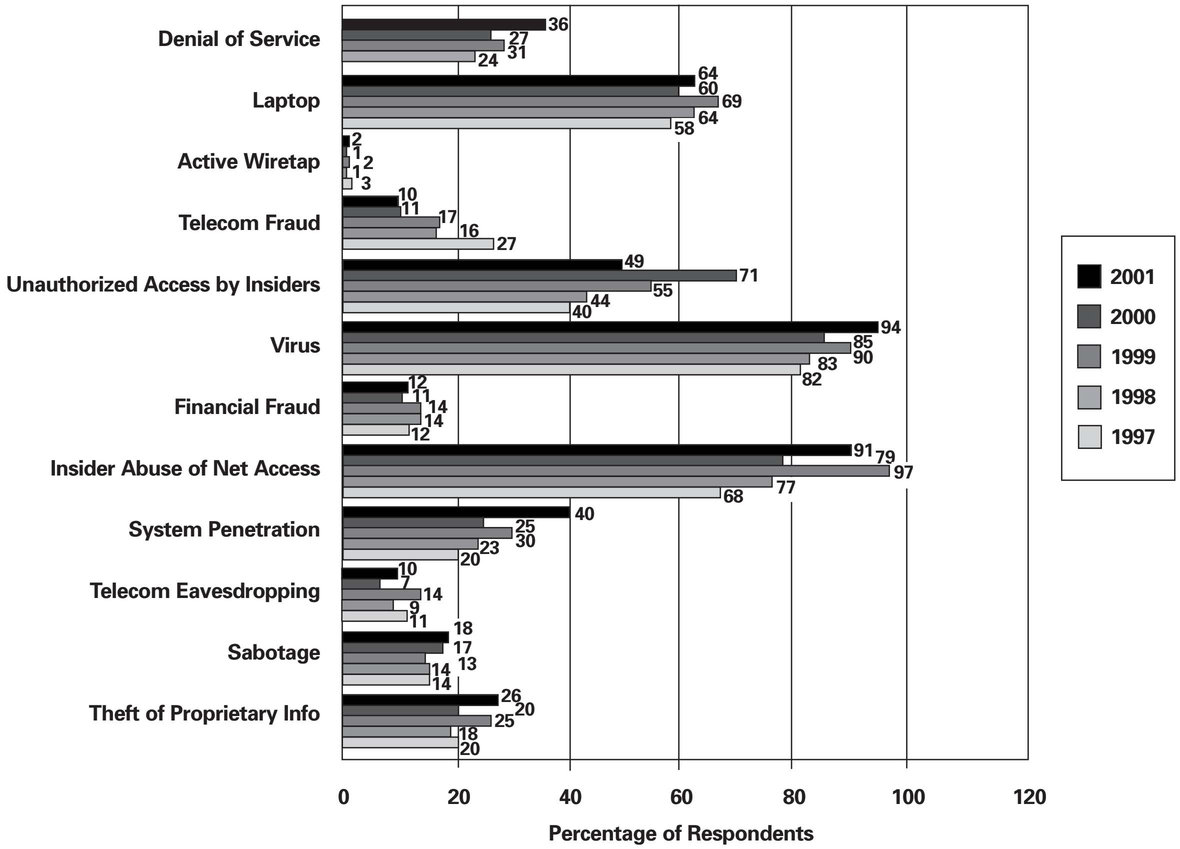
CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Note: In 2001, 78% of our survey respondents acknowledged financial losses, but only 37% of respondents could quantify the losses.

Average Losses					Total Annual Losses				
'97	'98	'99	'00	'01	'97	'98	'99	'00	'01
$954,666	$1,677,000	$1,847,652	$3,032,818	$4,447,900	$20,048,000	$33,545,000	$42,496,000	$66,708,000	$151,230,100
$164K	$86K	$163,740	$969,577	$199,350	$4,285,850	$2,142,000	$4,421,000	$27,148,000	$5,183,100
$45,423	$56K	$$76,500	$66,080	$55,375	$1,181,000	$562,000	$765,000	$991,200	$886,000
$132,250	$86K	$103,142	$244,965	$453,967	$2,911,700	$1,637,000	$2,885,000	$7,104,000	$19,066,600
$18,304	$56K	$93,530	$307,524	$357,160	$1,006,750	$3,720,000	$7,576,000	$27,984,740	$35,001,650
$957,384	$388K	$1,470,592	$1,646,941	$4,420,738	$24,892,000	$11,239,000	$39,706,000	$55,996,000	$92,935,500
n/a	$77K	$116,250	$108,717	$122,389	n/a	$2,787,000	$3,255,000	$$8,247,500	$4,283,600
$128K	n/a	n/a	n/a	n/a	$512,000	n/a	n/a	n/a	n/a
$75,746	$55K	$45,465	$180,092	$243,845	$12,498,150	$7,874,000	$5,274,000	$29,171,700	$45,288,150
$181,437	$2,809,000	$142,680	$ 1,124,725	$275,636	$3,991,605	$50,565,000	$3,567,000	$22,554,500	$6,064,000
$647,437	$539K	$26,655	$212,000	$502,278	$22,660,300	$17,256,000	$773,000	$4,028,000	$9,041,000
n/a	$49K	$20K	$5M	$0	n/a	$245,000	$20,000	$5,000,000	$0
$38,326	$32K	$86,920	$58,794	$61,881	$6,132,200	$5,250,000	$13,038,000	$10,404,300	$8,849,000
Total Annual Losses:					$100,119,555	$136,822,000	$123,799,000	$265,586,240	$377,828,700

Grand total of Losses reported (1997-2001): $1,004,135,495

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



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/83%
1997: 503 Respondents/89%

"Unfortunately, a lot of the confusion comes from the fact that some people keep quoting a 17-year old FBI statistic that indicated that 80 percent of all attacks originated from the inside. At the time this statistic was first released, it was almost certainly valid–the computing world at that time consisted to a large degree of mainframes and standalone PCs...Today we have a proliferation of network services (most notably worldwide web service) available to the entire Internet community–a truly target-rich environment for would-be attackers.

"One of the most revealing trends is the growing percentage of outsider-initiated attacks reported in the annual CSI/FBI survey. For the last few years, reported outside attacks have outnumbered reported insider attacks. I am, however, confident that despite the indication that external attacks now outnumber internal attacks, these surveys still under-represent externally initiated attacks...

"I'd like to add that any statistics concerning security-related incidents and computer crime are suspect and should not be taken at face value...

"What is the main point here?

"Is it that we should ignore the insider threat in favor of the outsider threat? On the contrary. The insider threat remains the greatest single source of risk to organizations...But what I am saying is that it is important to avoid underestimating the external threat. It is not only growing disproportionately, but it is being fueled increasingly by organized crime and motives related to espionage."

Net abuse is costly too

Of course, not all cyber crime involves trade secret theft, financial fraud or sabotage. Greed and revenge are not the only motives.

Some cyber crimes are crimes of passion. And, indeed, some security breaches are not even criminal in nature, but can nevertheless be costly due to lost productivity, civil liability damages, etc.

The number of respondents reporting employee abuse of network and Internet privileges (for example, downloading pornography or inappropriate use of e-mail systems) rose to 91% in 2001.

In '97, 68% reported Net abuse. In '99, reports of Net abuse spiked at 97% of respondents. In '00, only 79% detected Net abuse.

Meanwhile, the financial losses due to this problem cited by those respondents willing and/or able to quantify has risen steadily.

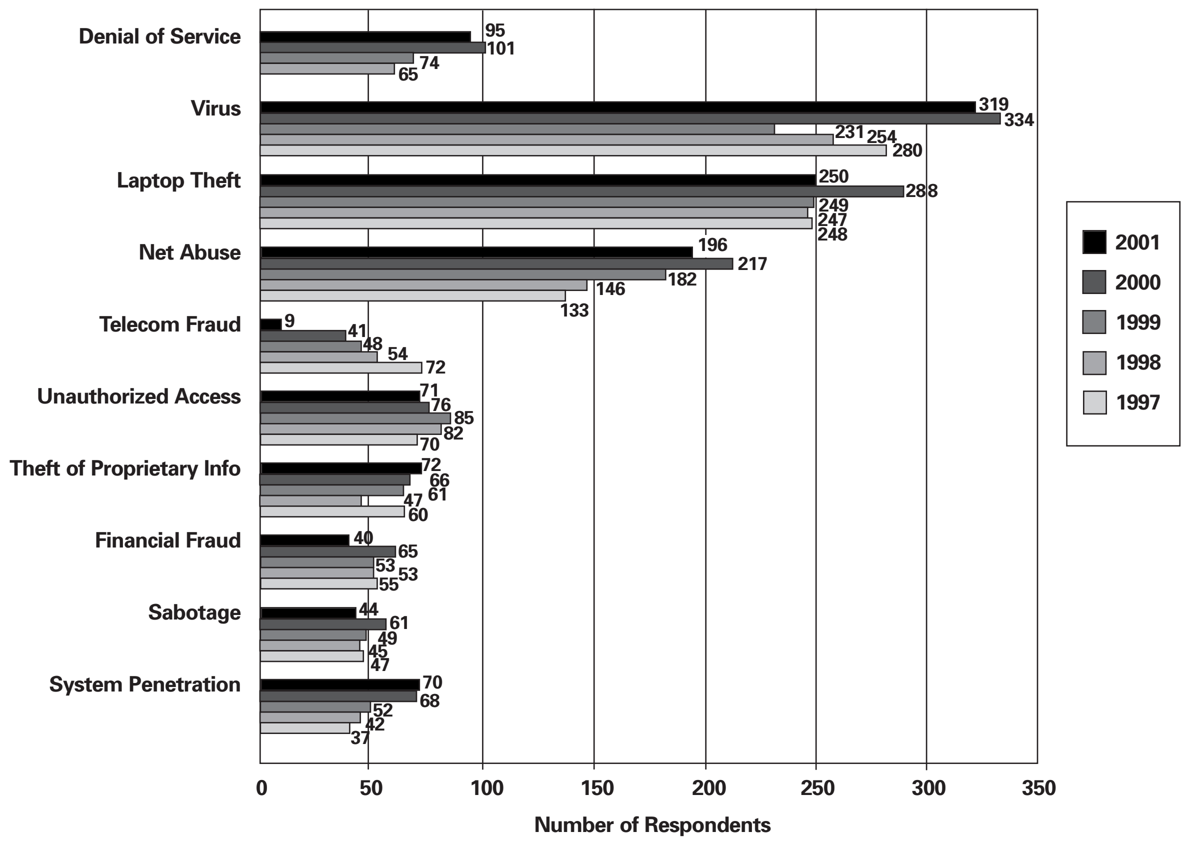
Organizations are cracking down.

A workplace privacy survey of human resources professionals at 722 companies, conducted by the Society for Human Resource Management and West Group, found that 74% monitor workers' Internet use at work; while 72% check on employees' e-mail and 51% review employees' phone calls.

In July 2000, Dow Chemical Co. fired 50 employees and disciplined 200 others after an e-mail investigation turned up hard-core pornography and violent subject matter. The violations were made by workers at all levels in the company. Dow's investigation was sparked by an employee complaint in May. The company does not monitor e-mail on a regular basis.

In Fall 2000, Dow Chemical fired a second group of workers

Financial Losses by Type of Attack or Misuse



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 344 respondents/64%
2000: 477 Respondents/74%
1999: 376 Respondents/73%
1998: 512 Respondents/98%
1997: 422 Respondents/75%

and reprimanded others after the employees allegedly violated the company's policies against pornographic e-mail. A month prior to the firings, Dow warned it would dismiss up to 40 people at a Texas facility in the wake of employee complaints about inappropriate e-mail usage.

But Dow wasn't the only major corporation to make news by giving people pink slips for prurient e-mail.

Twenty-three *New York Times* employees were fired at the Shared Services Center in Norfolk, VA, a hub for processing payroll, invoices and benefits. The fired employees "all transmitted clearly inappropriate and offensive material, which left no doubt as to the discipline required." Other employees received disciplinary warning letters. The NYT's e-mail policy says computers cannot be used to "create, forward or display any offensive or disruptive messages, including photographs, graphics or audio materials."

There were numerous other incidents that made ink.

Several former employees of Computer Associates International's Herndon, Virginia, office said they were fired over the holidays for sending sexually explicit e-mail.

First Union Corp., one of the nation's largest banks, fired seven employees for sending pornographic and other inappropriate e-mail.

Edward Jones, a large investment firm based in St. Louis, fired 18 employees, allowed one to resign and disciplined 41 others.

Cyber crime and infowar are global problems

Although only information security practitioners working in U.S.-owned corporations and government agencies are surveyed for our annual CSI/FBI study, both the burgeoning reality of cyber crime and the potential risks of infowar are global problems that demand global engagement. Not only does the trail of evidence in many of the high-profile cyber crimes documented in this report, as well as in *Tangled Web: Tales of Digital Crime* (ISBN:0-7897-2443-X), lead to other countries, but corporations and government agencies in those other countries have also been targeted.

Consider this random sampling of the many reports that I have received from around the world since just the beginning of the year.

According to Patrice Bergougnoux, a French law enforcement official in charge of statistics, there was an "explosion" in Internet crime, credit card fraud and mobile telephone fraud. French white collar crime, in general, rose 19% in 2000.

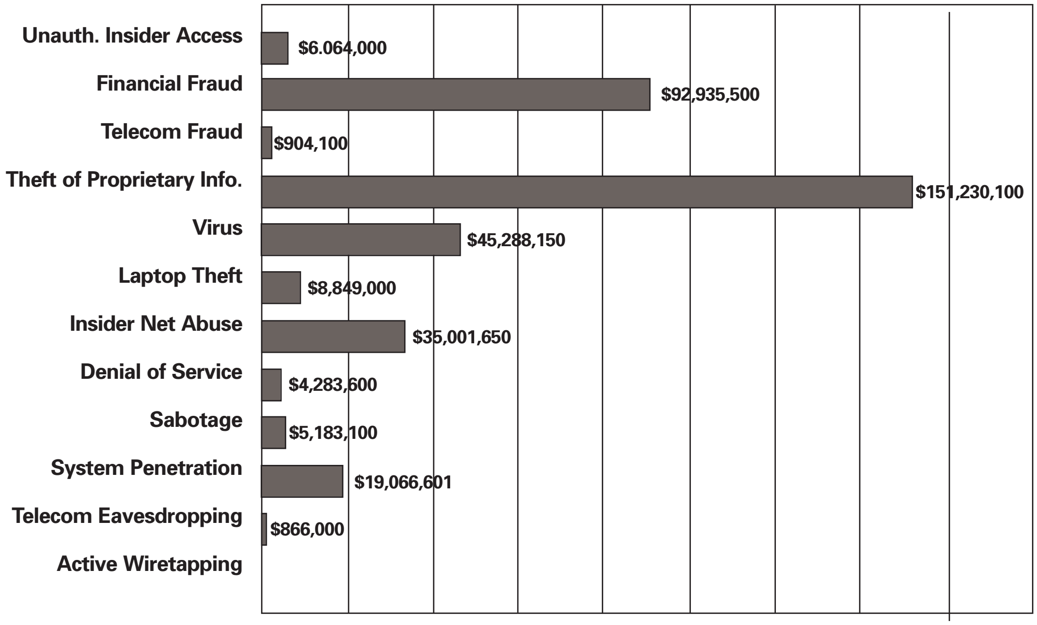
Two Indian computer trainers were arrested for allegedly trying to hack into the computers of the State Bank of India, the country's biggest commercial bank, and other state agencies.

The suspects allegedly sent e-mails in the name of Microsoft and Videsh Sanchar Nigam, India's monopoly overseas phone service provider, containing a file named Speed.exe.

When opened, it sent e-mails back to the accused giving them passwords and other data.

According to a study done by two Monterey, Mexico-based firms, Dreitech and Intermarket, ninety-five percent of the firms in a representative sample of Mexico's 500 leading companies have imperfect Internet security arrangements in place and feasibly

Dollar Amount of Losses by Type



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

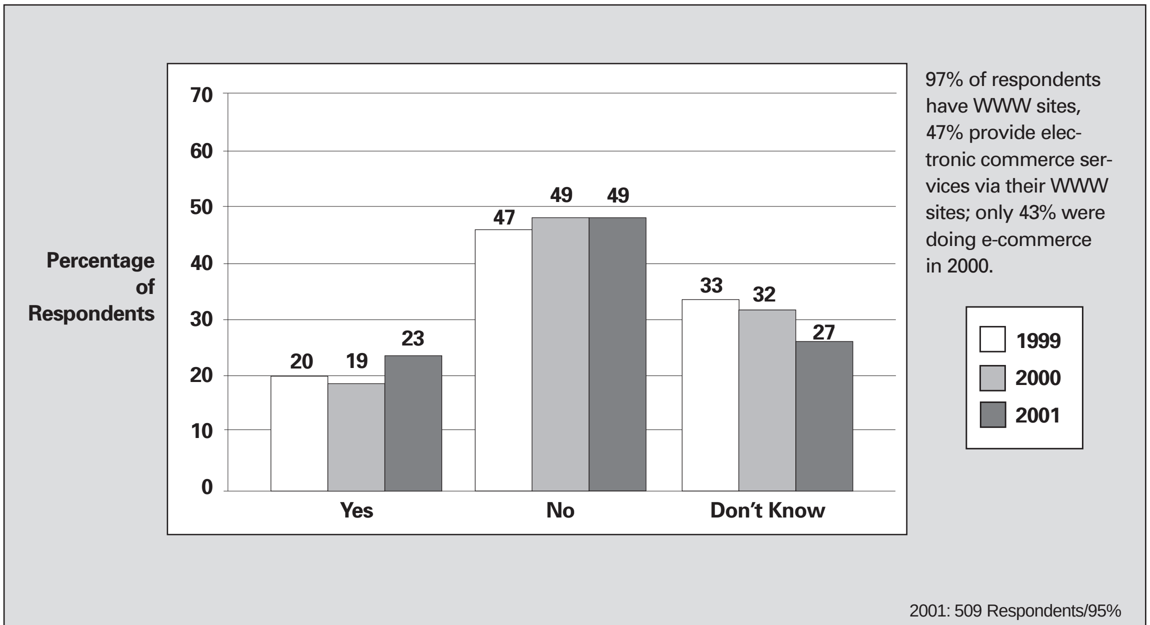
2001: 186 respondents/34%

could have their servers hacked. Among the companies the study identified as most vulnerable to attack by hackers was a leading Mexican bank.

According to ZD Net, a Romanian hacker launched a major distributed denial of service (DDoS) forcing one of the largest Internet Relay Chat (IRC) networks, Undernet, to shut down much of its service, system administrators said. One IRC server system administrator, who spoke on condition of anonymity, so that his servers would not become a target, said that the attacks appeared to be coming from hundreds of machines taken over by a single hacker based in Romania. He also suggested that Romania lacks the legal infrastructure to deal with attacks. “This is a big problem since the Romania hackers community is very active,” he says.

According to the Korea Information Security Agency (KISA), there were a total of 1,858 cases of hacking detected in Korea, as

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

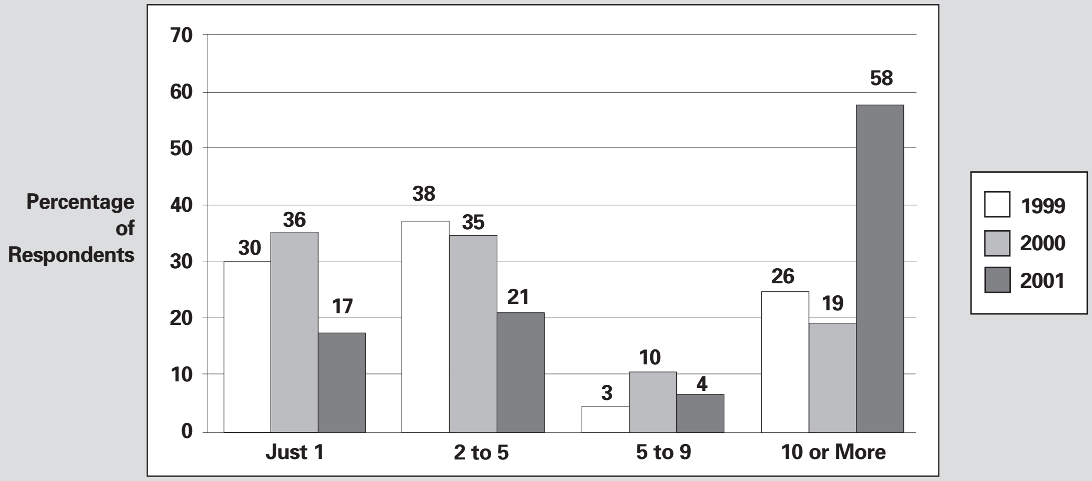


97% of respondents have WWW sites, 47% provide electronic commerce services via their WWW sites; only 43% were doing e-commerce in 2000.

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 509 Respondents/95%
2000: 603 Respondents/93%
1999: 479 Respondents/92%

WWW Site Incidents: If Yes, How Many Incidents?



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 211 Respondents/40%
2000: 120 Respondents/18%
1999: 92 Respondents/18%

of November 2000, more than triple the 527 cases found in 1999. KISA said that corporations were the main target of attacks.

Con men succeeded in stealing credit card numbers and other information from 10,000 Web surfers with a fake e-mail asking them to re-register with Brazil's biggest Internet portal. An e-mail sent in September to clients of Universal Online (UOL) tricked them into filling out a form on a fake registration site, a note on the UOL site said. "This was one of the biggest coups on the Brazilian Internet that we know of and that we can explain," said Renato Funicello, police director of information technology.

There is a global economy, and cyberspace too is global. There is, therefore, an urgent need for international cooperation on the 21st century problems such cyber crime and information warfare.

The Council of Europe's "Draft Convention of Cybercrime" (http://conventions.coe.int/treaty/en/projets/cybercrime.htm) has been met with opposition, as Dr. Denning explains.

"The CoE Cybercrime Convention could help facilitate the fight against cybercrime by promoting more uniform laws and better cooperation among nations signing the treaty. However, it has raised significant issues regarding privacy and corporate liabilities and responsibilities. The draft has been criticized for failing to provide adequate privacy protections regarding access to stored data and electronic surveillance and for potentially burdening industry with costly requirements to implement electronic surveillance, retain evidence, and respond to a potentially huge number of subpoenas and court orders from foreign governments. Industry is also concerned about liabilities for actions taken on their networks in violation of laws stemming from the treaty. An earlier draft raised concerns about whether it could lead to laws prohibiting the development or use of hacking tools for research purposes and to test the security of one's own systems, but the most recent draft clarifies that that is not to be the case."

I hope those rightfully concerned about the rule of law, particularly international law, in cyberspace and those rightfully concerned about the privacy of the individual in cyberspace can find common ground.

Prior to March 2001, many environmentalists criticized the Kyoto accords on "Global Warming," negotiated during the Clinton-Gore administration, as too weak. Well, I imagine that they would prefer the Kyoto accords as agreed upon to the Bush-Cheney administration's unilateral decision to renege on the U.S. commitment and walk away from the treaty.

Those in government, industry and privacy advocacy working on developing the cybercrime treaty must put the common good, the greater goal, ahead of lesser considerations.

(Of course, if the global environment is allowed to deteriorate too far too fast, progress made on security and privacy in cyberspace really won't matter too much.)

To report or not to report

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.

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

In 1999 survey, 32% answered that they had reported such incidents to law enforcement. A positive step forward.

In 2000, the percent of respondents who reported intrusions to law enforcement dropped to 25%.

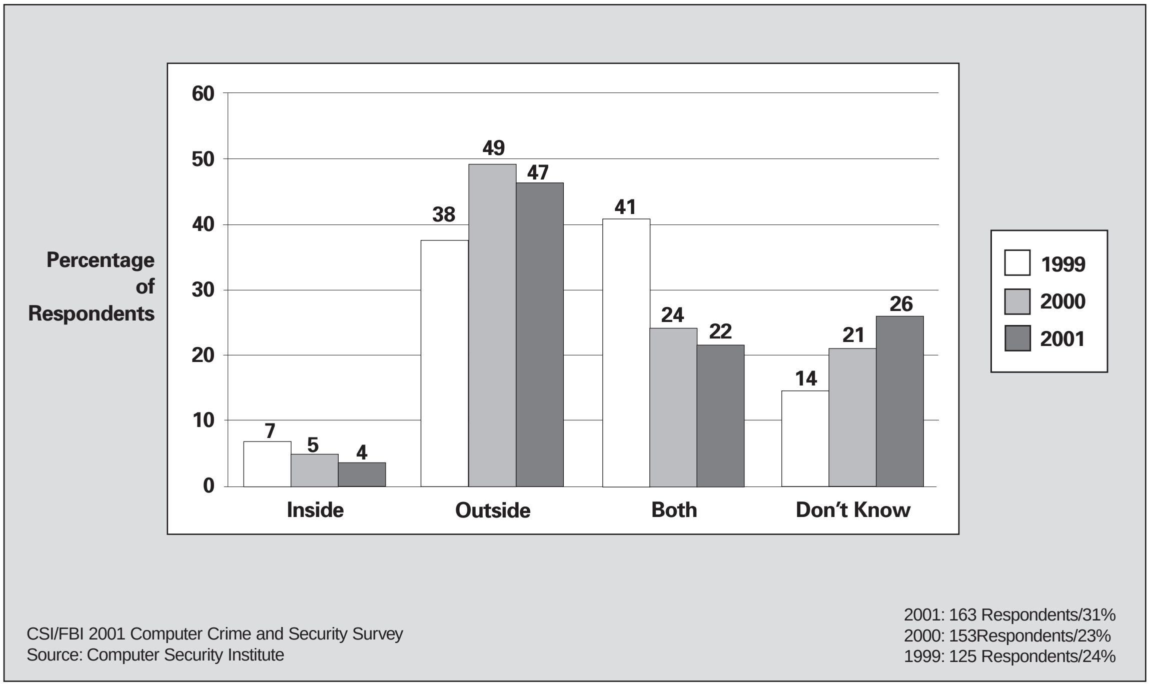
In 2001, the percent of those who reported intrusions to law enforcement rose again to 36%.

The trend is upward.

Dr. Denning cites some reasons for the increase.

"Many attacks are highly visible, e.g., Web defacements and denial-of-service attacks, so it is harder to conceal an attack. Also, law enforcement agencies are getting better at investigating cyber incidents, so victims might have greater confidence in their ability to

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



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 163 Respondents/31%
2000: 153Respondents/23%
1999: 125 Respondents/24%

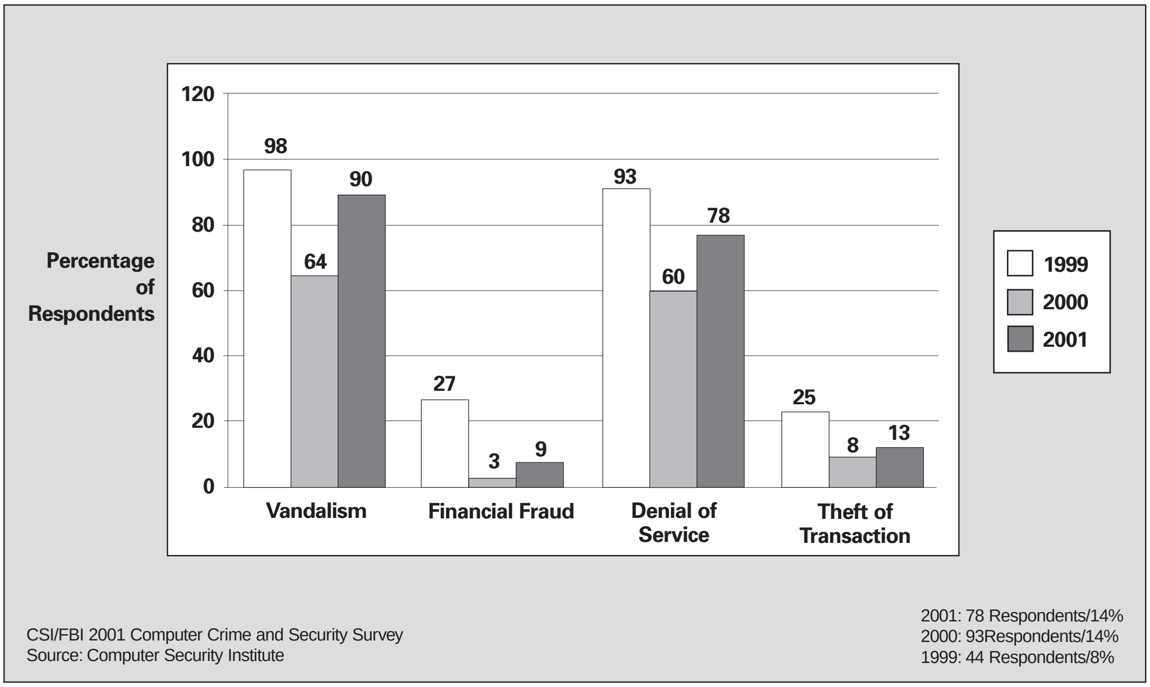
handle their cases effectively. However, concern over negative publicity remains a strong deterrent to reporting."

The truth is out there
The CSI/FBI Computer Crime and Security Survey is a non-scientific, informal but narrowly focused poll of information security practitioners. Its aim is to heighten security awareness, promote information protection, and encourage cooperation between law enforcement and the private sector.

The survey is at best a series of snapshots that give some sense of the "facts on the ground" at a particular time. The findings are in large part corroborated by data from other reputable studies, as well as by real-world incidents documented in open source publications. I also suggest that the findings of the CSI/FBI survey are strengthened by having six straight years of data to draw on.

Every year, with each new version of *Issues and Trends,* I try to lay this caveat out as best I can. For example, in 1999, I included a passage from Donn B. Parker's excellent book, *Fighting Cyber*

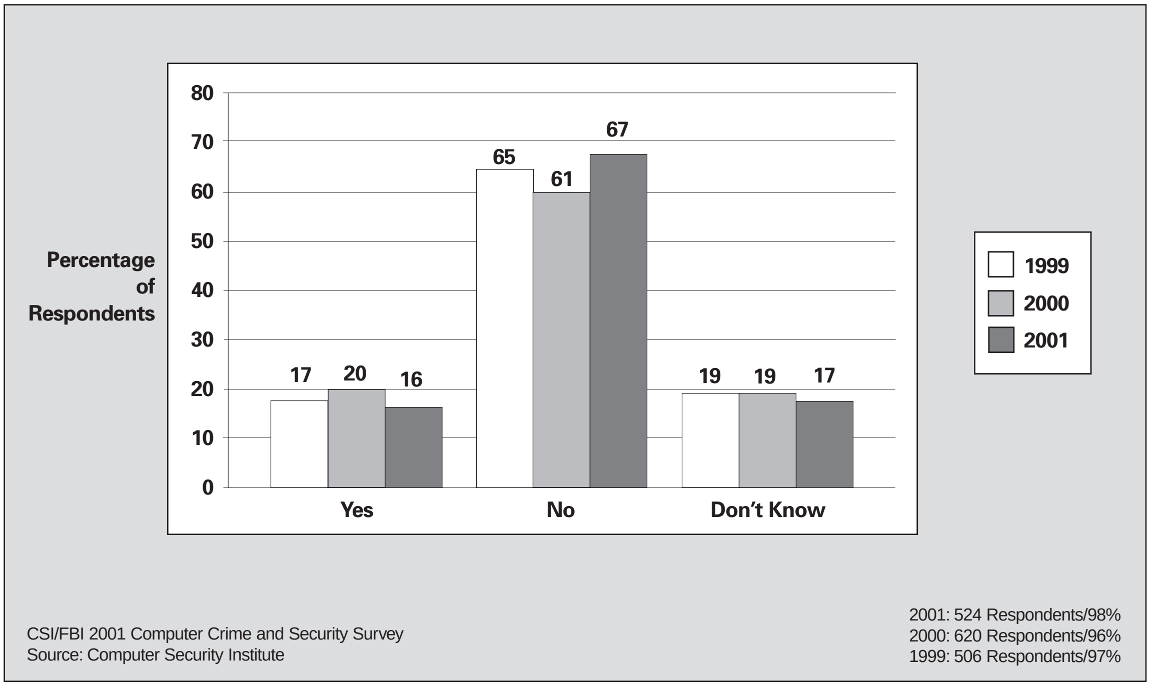
WWW Site Incidents: What Type of Unauthorized Access or Misuse?



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 78 Respondents/14%
2000: 93Respondents/14%
1999: 44 Respondents/8%

Would Your Organization Consider Hiring Reformed Hackers as Consultants?



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 524 Respondents/98%
2000: 620 Respondents/96%
1999: 506 Respondents/97%

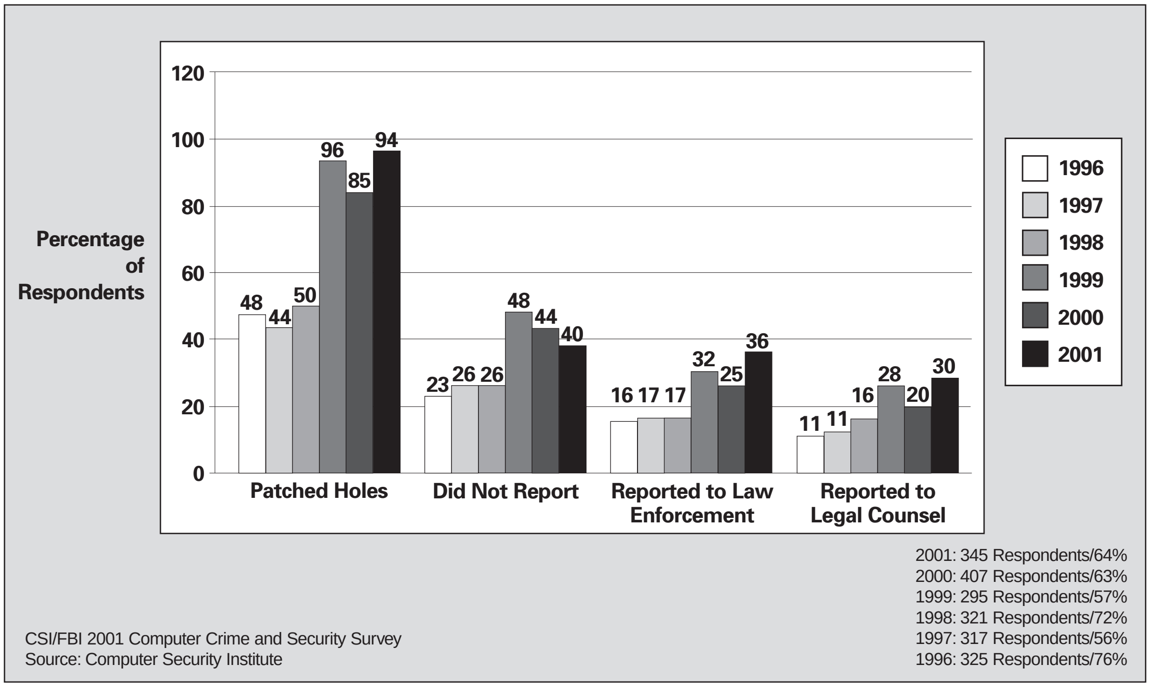
Crime: A New Framework for Protecting Information (ISBN: 0-471-16378-3), in which Parker (one of the heroes of information security) rightfully rails against cyber crime "statistics."

This year, I urge you to consider Bruce Schneier's balanced view, excerpted from *Cryptogram,* as you evaluate the data.

"The results are not statistically meaningful by any stretch of the imagination—they're based on about 500 survey responses each year—but it is the most interesting data on real world computer and network security that we have. And the numbers tell a coherent story. (I'm just going to talk about the 2001 numbers, but the numbers for previous years track pretty well.)

"This data is not statistically rigorous, and should be viewed as sus-

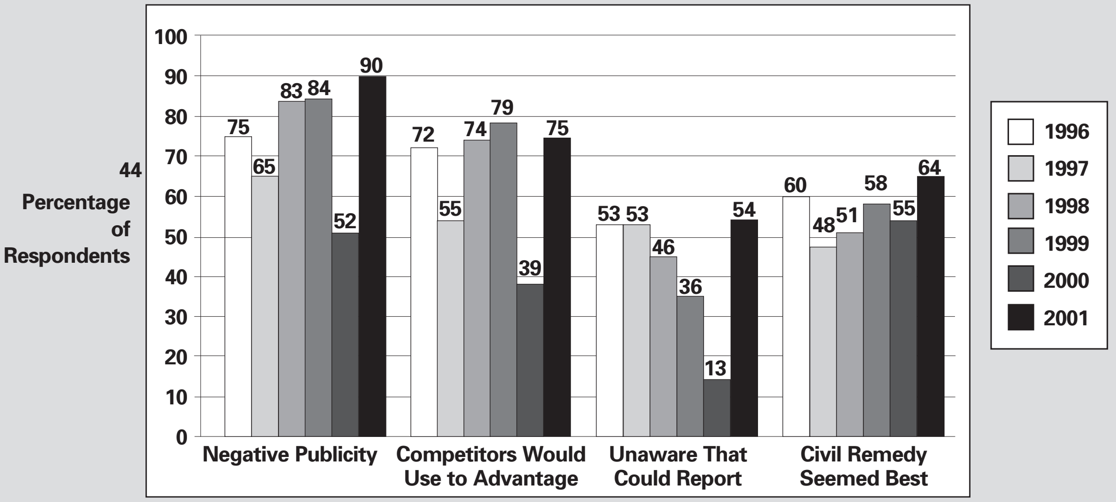
If Your Organization Has Experienced Computer Intrusion(s) Within the Last 12 Months, Which of the Following Actions Did You Take?



2001: 345 Respondents/64%
2000: 407 Respondents/63%
1999: 295 Respondents/57%
1998: 321 Respondents/72%
1997: 317 Respondents/56%
1996: 325 Respondents/76%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

The Reasons Organizations Did Not Report Intrusions to Law Enforcement



2001: 151 Respondents/28%
2000: 209 Respondents/32%
1999: 107 Respondents/20%
1998: 96 Respondents/19%
1997: 142 Respondents/25%
1996: 64 Respondents/15%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

pect for several reasons. First, it's based on the database of information security professionals that the CSI has, self-selected by the 14% who bothered to respond. (The people responding are probably more knowledgeable than the average sysadmin, and the companies they work for more aware of the threats. Certainly there are some large companies represented here.) Second, the data is not necessarily accurate, but only the best recollections of the respondents. And third, most hacks still go unnoticed; the data only represents what the respondents actually noticed.

Even so, the trends are unnerving. It's clearly a dangerous world, and has been for years. It's not getting better, even given the widespread deployment of computer security technologies. And it's costing American businesses billions, easily."

The CSI/FBI survey results should be taken, in my opinion, as raw intelligence (something that some companies are trying to charge you a lot of money for). They should not be used as the basis for actuarial tables or sentencing guidelines. They should not be used as a basis to extrapolate some pie in the sky numbers on intrusions or financial losses for the whole economy or the whole of the Internet. They should be used as an intelligence resource for your own thinking about the emerging trends in cyber crime. Nothing more, nothing less.

CSI offers the survey results as a public service. The report is free to anyone who requests a copy. The participation of the FBI's San Francisco office has been invaluable. They have provided input into the development of the survey itself 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 foots the bill for the project, and is solely responsible for the results.

A note on methodology

Questionnaires with business reply envelopes were sent by U.S. post ("snail mail") to 3,900 information security professionals; 538 responses were received for a 14% response rate.

In 2000, 643 responses were received (15%). In 1999, 521 responses were received (14% of 3,670 questionnaires sent). In 1998, 520 responses were received (13% of 3,890 questionnaires sent). In 1997, 563 responses were received (11.49% of 4,899 questionnaires sent). In 1996, 428 responses were received (8.6% of 4,971 questionnaires sent).

The responses were anonymous.

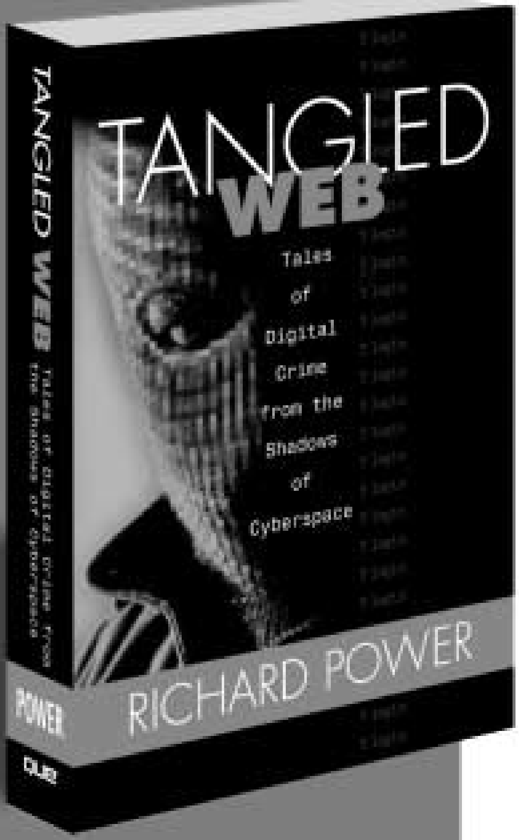
Job titles of those queried range from information security manager to data security officer to senior systems analyst.

Organizations surveyed included corporations, financial institutions, government agencies and universities in the U.S. only.

Who to Call

For referrals on specific criminal investigations:
Chris Beeson, Special Agent,
San Francisco FBI Computer Crime Squad,
22320 Foothill Blvd., Hayward, CA. 94541,
Ph: 510-886-7447, Fax: 510-886-498,
E-mail: nccs-sf@fbi.gov
For general information, go to http://www.nipc.gov

For information on the CSI/FBI study:
Richard Power, Editorial Director,
Computer Security Institute,
600 Harrison Street, S.F., CA. 94107,
Ph: 415-947-6371, Fax: 415-947-6023,
E-mail: rpower@cmp.com
For general information, go to http://www.gocsi.com


TANGLED WEB
Tales of Digital Crime from the Shadows of Cyberspace
RICHARD POWER
TANGLED WEB Tales of Digital Crime from the Shadows of Cyberspace
POWER
QUE

You are the TARGET

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 is dedicated to advancing the view that information is a critical asset that must be protected. CSI members share expertise and experience to protect their organizations from any and all possible threats and disasters through training, education and proactive security programs. The goal of CSI is the professional development of its members through high-quality publications, educational opportunities and networking. As a member of CSI you are linked to a high-powered information source and an organization dedicated to providing you with unlimited leadership development in one package. For more information, fax this form to 415.947.6023 or call 415.947.6371.

You need resources

Conferences

28th Annual Computer Security Conference & Exhibition
October 29-31, 2001, Washington, DC
The world's largest conference devoted to computer and information security

NetSec 2002
June 17-19, 2002, San Francisco, CA
An in-depth program tailored to help you build and maintain secure networks

Training:

- Windows NT
- Risk Analysis
- Intra/Internet
- Awareness
- Intrusion Management
- Networks

Publications:

Computer Security Alert (10 page monthly newsletter)
Computer Security Journal (quarterly)
Annual Computer Security Products Buyers Guide
Current & Future Danger: A Primer on Computer Crime & Information Warfare
Information Protection Assessment Kit
FrontLine
and more

Name ____________________

Organization ____________________

Address ____________________

City ________ State ________ Zip ________ Country ________

Phone ____________ Fax ____________

IT99

Visit us on the world wide web:

http://www.gocsi.com