CSI
COMPUTER SECURITY INSTITUTE

COMPUTER SECURITY ISSUES & TRENDS

VOL.VIII, NO.1 SPRING 2002

2002 CSI/FBI Computer Crime and Security Survey

By Richard Power

The "Computer Crime and Security Survey" is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States.

Now in its seventh 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 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2002 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

Patrice Rapalus, CSI Director, remarks that the "Computer Crime and Security Survey," has served as a reality check for industry and government:

"Over its seven-year life span, the survey has told a compelling story. It has underscored some of the verities of the information security profession, for example that technology alone cannot thwart cyber attacks and that there is a need for greater cooperation between the private sector and the government. It has also challenged some of the profession's 'conventional wisdom,' for example that the 'threat from inside the organization is far greater than the threat from outside the organization' and that 'most hack attacks are perpetrated by juveniles on joy-rides in cyberspace.' Over the seven-year life span of the survey, a sense of the 'facts on the ground' has emerged. There is much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly and commonplace."

The FBI's Executive Assistant Director (EAD) Bruce J. Gebhardt, former Special Agent-in-Charge FBI San Francisco, stresses the need for the cooperation between government and private sector that the survey project reflects.

"The United States' increasing dependency on information technology to manage and operate our nation's critical infrastructures provides a prime target to would-be cyber-terrorists. Now, more than ever, government and private sector need to work together to share information and be more cognitive of information security so that our nation's critical infrastructures are protected from cyber-terrorists."

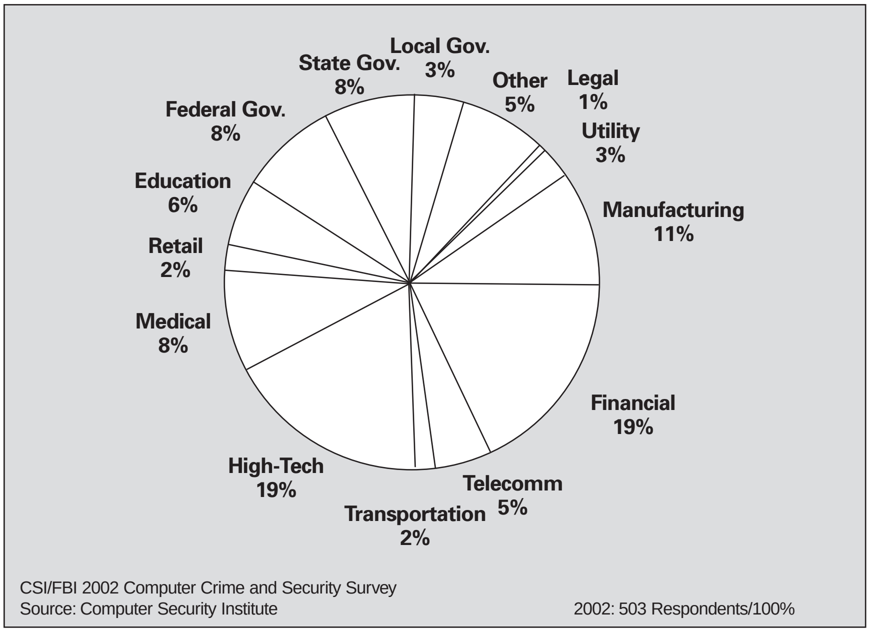
The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established the National Infrastructure Protection Center (NIPC) located at FBI headquarters and the Regional Computer Intrusion Squads located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

Respondents by Industry Sector



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

Briefing notes

Seven is a sacred number for many mystical traditions, it is also a lucky number for many gamblers. For me, seven, i.e. the number of years we have conducted the CSI/FBI Computer Crime and Security Survey, is a moment to pause and ponder the life of the project.

In mid-1995, CSI started the survey in collaboration with two foresighted FBI veterans, George Vinson, now Homeland Security Director for Governor Gray Davis (D-CA), who was then in charge of the fledgling San Francisco Computer Crime Squad and Pat Murphy, now with Charles Schwab, one of Vinson's agents who served as liaison with CSI.

Much has happened since then–the Nunn Senate hearings of Security in Cyberspace; the establishment of the National Infrastructure Protection Center (NIPC); the issuance of Presidential Decision Directive 63 (PDD63); the signing into law of the Economic Espionage Act (EEA). And so much more.

Here are the results of the seventh annual survey, together with some insights from subject matter experts, as well as a few of my own comments. If the survey continues beyond the seven-year cycle it has now completed, it will be designed differently and reflect new priorities.

But it has certainly met its objectives to raise the level of security awareness throughout the world, help determine the scope of computer crime, foster cooperation between federal law enforcement and the private sector and promote sound information security practices within organizations.

Who we asked

Most respondents work for large corporations. The heaviest concentrations of respondents are in the high-tech (19%) and financial services (19%) sectors. Manufacturing is the next largest industry segment (11% of respondents).

Federal (8%) state (8%) and local (3%) government agencies, taken together, comprise 19% of respondents.

Organizations in other vital areas of the national infrastructure also responded—for example, medical institutions (8%), telecommunications (5%) and utilities (3%).

The responses come from organizations with large payrolls—for example, 24% reported 10,000 or more employees and 12% reported from 5,001 to 9,999 employees.

Thirty-seven percent of respondents in the commercial sector reported a gross income over $1 billion, 8% reported gross income of from $501 million to $1 billion, and 16% reported gross income of from $100 million to $500 million.

As I have mentioned before, don't be dissuaded by the fact that only 503 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 recent economic downturn.

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 seven-year life of the survey confirm, have the potential to do serious damage to U.S. economic competitiveness.

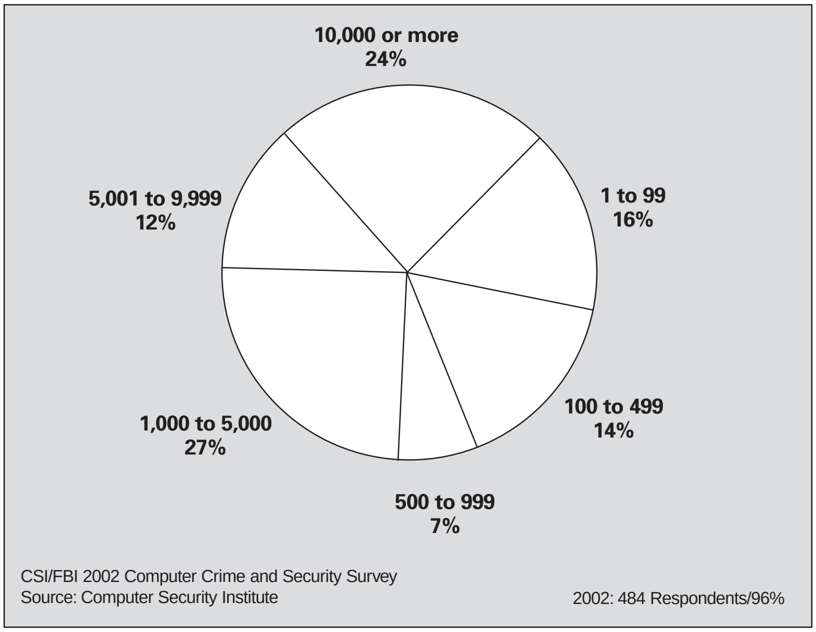
Unless information security is the focus of concerted efforts throughout both the public and private sector, the rule of law in cyberspace, as well as U.S. leadership in the global marketplace will be undermined.

What they used

For the fifth year in a row, we asked what kind of security technologies respondents were using. And, as we have discussed in previous years, the results were compelling.

For example, although 89% of respondents have firewalls and 60% use IDS, 40% report system penetration from the outside; and although 90% of respondents use anti-virus software, 85%

Respondents by Number of Employees



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

of them were hit by viruses, worms, etc.

Every year, I receive hundreds of requests for permission to reproduce the data in the "CSI/FBI Computer Crime and Security Survey" in books, reports, magazine articles, and yes, security technology vendor sales presentations.

Perhaps if I insisted that the security technology vendors who want to include the data on types of attack and financial losses in their sales presentations also include the data on types of security technology used, I imagine that their penchance for using the CSI/FBI study results might wane to some extent.

Some IT analysts have predicted that security technologies will become appliances, i.e., products that you can just plug in and forget about. Well, you can just plug something in and forget about it. But you won't necessarily have reduced your vulnerability.

Information security requires a whole-hearted organizational commitment of resources (financial, human and technological) to an enterprise-wide program designed to evolve and adapt to new dangers. But most people are looking for a quick fix.

Consider biometrics and PKI. Both of these technologies are important. Both have great potential. But the hype surrounding them (particularly the hype surrounding biometrics after 9/11) would lead you to believe that one or the other would dispel the whole of the digital shadow simply by being deployed.

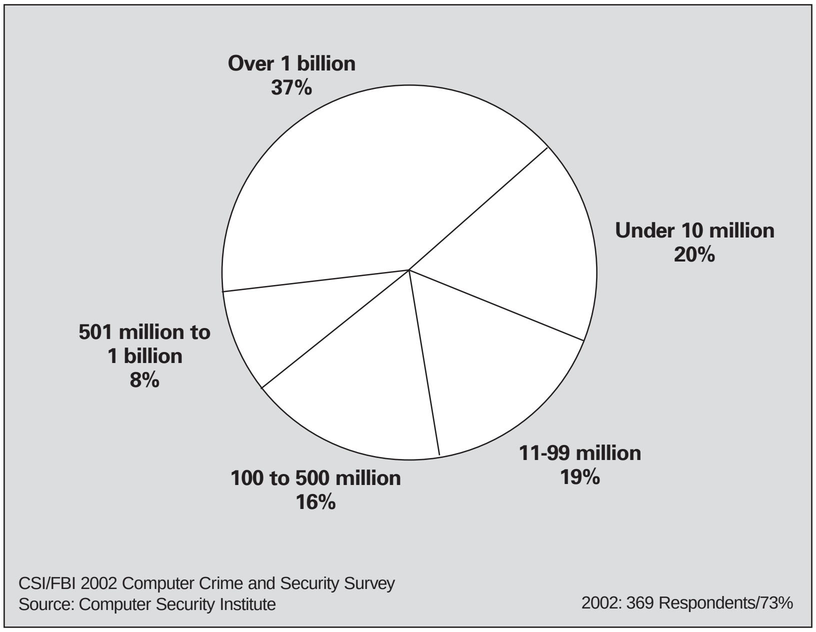
Gene Spafford, Director of CERIAS at Purdue University, brings some sanity to bear on biometric technology.

"Biometrics are being misrepresented or are simply misunderstood. There are three basic, independent but related concepts: identification, authentication, and authorization—who you are, proving who you are, and determining what you are allowed to do. Many of the biometrics methods being presented as "solutions" to security questions have been designed as only authentication systems. Given a set of individuals, they can confirm with high confidence that a person matches one of the stored profiles. Examples include matching fingerprints or facial features in a database. The problem is that you need a lot of detail with some of these to prevent false matches, and in some cases there hasn't been the kind of wide-scale study necessary to determine overall accuracy in a large population. Thus, using these mechanisms for identification may not be as foolproof or error-resistant as we need. Furthermore, there is the underlying fallacy that authenticating an identity confers authorization. That we can match someone's facial features or hand geometry to a stored value in an ID database does not mean the person is "safe" or should be automatically authorized to do something (e.g., get on a plane with only a cursory search). Every criminal and terrorist will have at least one ID (maybe more if they subvert the database or bribe an employee), but prior to a first offense they won't be known as a problem. All of the 9/11 hijackers had valid IDs and they did little to hide their identities. If there was facial recognition at the airports, and each one matched fingerprints and retinal scans against a high-tech ID card, the biometric authentication wouldn't have changed the outcome. Knowing who someone is doesn't tell us what they're going to do! Security comes from understanding systems, goals, and methods. Strong tools applied in the wrong way for the wrong reasons don't help, and may even confound other defenses. For instance, imagine if some people have strong biometric IDs and others don't. Do you think guards will search them all equally at the airport? The terrorists and criminals may be among the first to get new IDs with biometrics—it may help them lull suspicion! Airports might be better off if there were NO IDs so that the guards stay suspicious of everyone!"

And what about PKI? Gene Schultz, CISSP, of University of California Berkeley Laboratory laments.

"PKI is truly a sad issue. PKI has been held up as a panacea, and perhaps it is, but the PKI movement has fizzled badly. Just a few weeks ago I read a research survey that indicated that only one percent of corporations in the financial arena actually use PKI software. I cannot confirm the accuracy of this statistic, but I can say with confidence that during the nine years I served as a consultant to industry, I did not see many successful PKI deployments. The normal course of events was for an organization to design a PKI, purchase the necessary software and hardware, and then decide not to use the PKI capability that it had developed. No, as things are currently going, PKI is (with a few very notable exceptions) not buying us much, and

Respondents by Gross Income



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

I am not sure if it is going to serve us much better in the future. At a minimum, organizations and the public need to understand what public key cryptography is and how it can help if PKI technology is ever going to be widely accepted and used.

The trends continue

Highlights of the "2002 Computer Crime and Security Survey" include the following:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.
- As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).
- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- Thirty-four percent reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

Respondents detected a wide range of attacks and abuses:

- Forty percent detected system penetration from the outside.
- Forty percent detected denial of service attacks.
- Seventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).
- Eighty-five percent detected computer viruses.

WWW crime has become commonplace

For the fourth year in a row, we asked our respondents some questions about their WWW sites.

Here are the results:

- Ninety-eight percent of respondents have WWW sites.
- Fifty-two percent conduct electronic commerce on their sites.
- Thirty-eight percent suffered unauthorized access or misuse on their Web sites within the last twelve months. Twenty-one percent said that they didn't know if there had been unauthorized access or misuse.
- Twenty-five percent of those acknowledging attacks reported from two to five incidents. Thirty-nine percent reported ten or more incidents.
- Seventy percent of those attacked reported vandalism.
- Fifty-five percent reported denial of service.
- Twelve percent reported theft of transaction information.
- Six percent reported financial fraud.

WWW crimes range from cyber-vandalism (e.g. Web site defacement) at the low end to theft of proprietary information and financial fraud at the high end.

Despite a brief decline in the weeks after 9/11, Web site defacements, the most prevalent form of cyber vandalism, increased globally during 2001, according to Mi2g (www.mi2g.com).

The monthly high was in May (3,853 sites defaced), says Mi2g; the monthly low was in September (812 sites defaced).

Mi2g also reports that ".com" domains were the targets of almost 30% (8,736) of all Web site defacements (30,388), during the year.

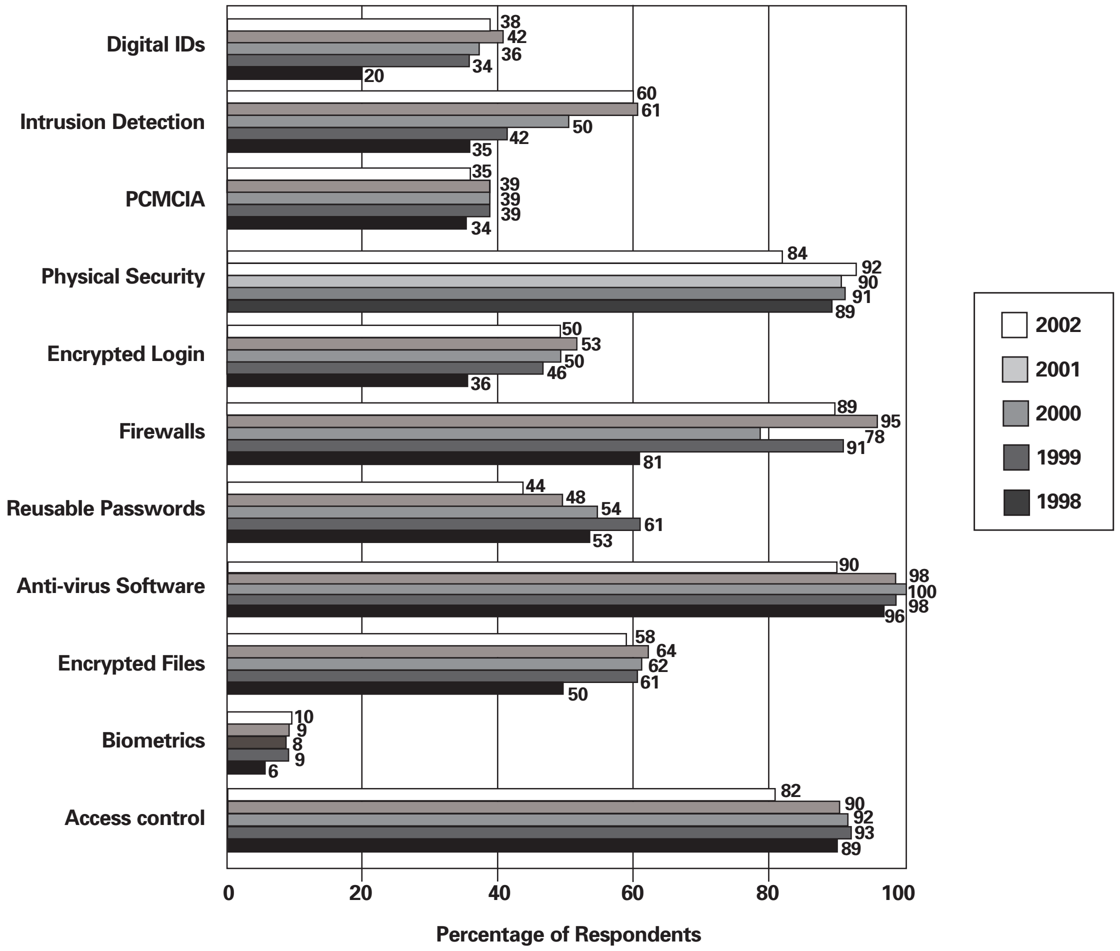
The next most frequently defaced site domain names were China's ".cn" and Taiwan's ".tw," which together accounted for 2,653 Web site defacements, or almost 9 percent of the global total.

The ".gov" domains experienced a 37% increase in Web site defacements—from 181 to 248 —during 2001, while ".mil" domains saw a 128% increase in defacements during the same period.

Israel's ".il" domain name groups during 2001—up 220% to 413 defacements during the year.

India's ".in" domain defacements rose by 205% to include 250 sites, while Pakistan's ".pk" domain defacements increased 300% to 82 during the year.

Security Technologies Used



CSI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

2002: 500 Respondents/99%
2001: 530 Respondents/99%
2000: 629 Respondents/97%
1999: 501 Respondents/96%
1998: 512 Respondents/98%

Web site defacements in the British "gov.uk" top level domain increased 378% from 9 in 2000 to 43 in 2001.

Clearly, much of this intense activity involves hacktivism related to geopolitical conflicts in the Middle East, the Indian Subcontinent and the Straits of Taiwan. But political activism isn't the only motivation for cyber-vandalism. Some of it is the acting out of personal grudges; some of it is simply random.

Of course, theft of proprietary information and financial fraud, although less frequent, are much more serious problems. Here are two stories that illustrate just a few of the many problems that have surfaced during the last year.

In February 2002, Kevin Poulson of *Security Focus* reported that security holes in the *New York Times* internal network left sensitive databases exposed to hackers, including a file containing Social Security numbers and home phone numbers for contributors to the Times op-ed page.

"In a two-minute scan performed on a whim, twenty-one-year-old hacker and sometimes-security-consultant Adrian Lamo discovered no less than seven misconfigured proxy servers acting as doorways between the public Internet and the Times' private intranet, making the latter accessible to anyone capable of properly configuring their Web browser.

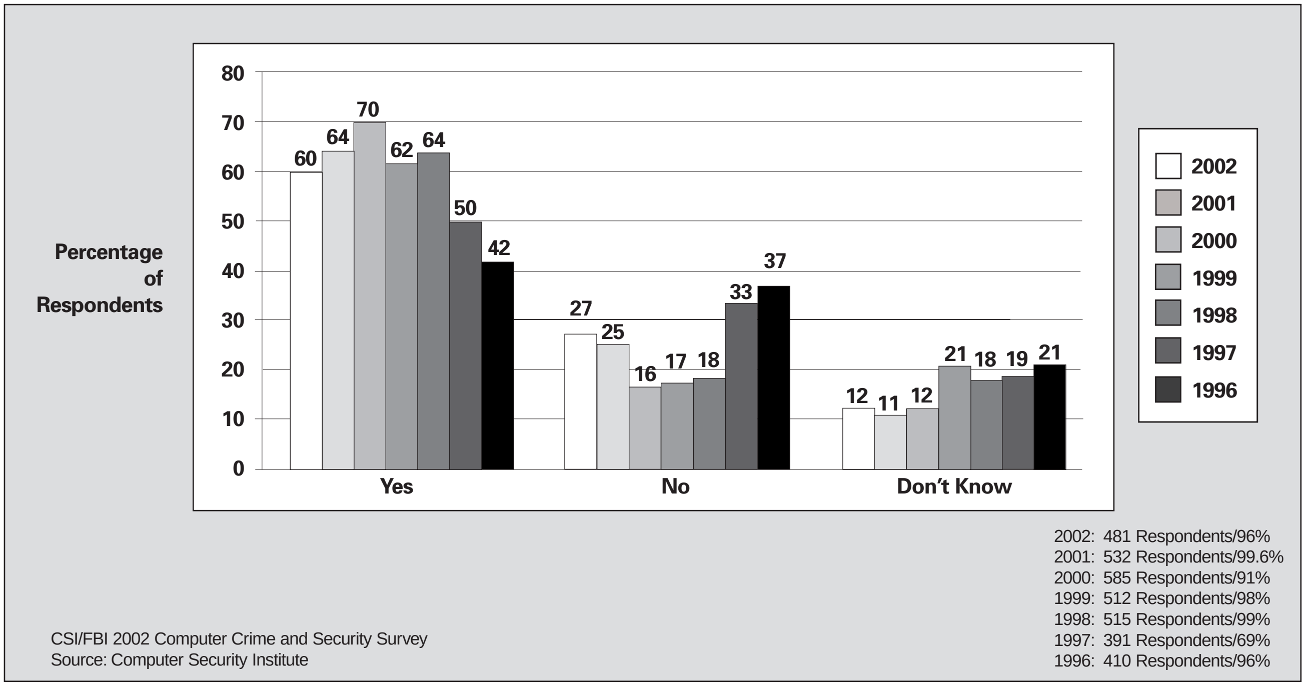
"Once on the newspaper's network, Lamo exploited weaknesses in the Times password policies to broaden his access, eventually browsing such disparate information as the names and Social Security numbers of the paper's employees, logs of home delivery customers' stop and start orders, instructions and computer dial-ups for stringers to file stories, lists of contacts used by the Metro and Business desks, and the 'WireWatch' keywords particular reporters had selected for monitoring wire services."

In May 2001, MSNBC reported a devastating bug had been found in shopping cart software called "PDG" that exposed all customer records on about 4,000 Web sites. The FBI issued a public warning directed to the software's customers, but a small e-commerce Web site named SawyerDesign.com didn't notice.

"Within days, computer criminals had a field day, racking up thousands of dollars of charges on victims' cards at gambling sites, buying phone cards and downloading pricey software.

"But SawyerDesign.com's operators, Regal Plastic Supply, never received the e-mail (warning of the danger) because it bought the software from a reseller. It is also easy to understand how Regal never

Unauthorized Use of Computer Systems Within the Last 12 Months



2002: 481 Respondents/96%
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 2002 Computer Crime and Security Survey
Source: Computer Security Institute

noticed the warning on the FBI's National Infrastructure Protection Center (NIPC) Web site.

"And since the company garners only a trickle of transactions from the sports memorabilia display case site–its main business is real-world plastic supply–it's not surprising that the firm doesn't have a full-time system administrator applying patches to the $1,000 shopping cart software."

Two months later, MSNBC reported that despite warnings about the dangers and a patch being made available, the exploitation of the PDG hole had become commonplace.

"Time has apparently run out for Internet e-commerce sites to fix a critical software flaw that exposes customer credit card numbers. In the past few days, dozens of URLs have been posted in Internet chat rooms linking to small Web sites that hadn't patched their flawed shopping cart programs. The flaw is so widespread that some of the URLs containing customer information are being picked up by search engines—meaning finding hot cards is almost as easy as conducting a search on Yahoo or Google.

"While hundreds of sites have downloaded and installed the necessary patch provided by software maker PDG Software Inc., dozens of others have yet to do so.

"And now, instructions on how the flaw works have spread through the Internet's underground, and exploiting it is so trivial that several sites are being victimized each day."

The biggest problem in this area of course, is the theft of large quantities of credit card records from ill-protected servers. This particular kind of heist has become the 21st century equivalent of the armored car robbery.

Rik Farrow, who teaches CSI's course on "Intrusion Detection, Attacks and Countermeasures," comments.

"What is common to many e-commerce sites is the use of credit cards for financial transactions. Credit card information is the single, most commonly traded, financial instrument for attackers. They can sell credit card info, use it to buy themselves new computers and equipment, trade it for other information, etc. The point is simply: any data that has any value must not be stored on public Web servers. The Web server should communicate, as carefully as possible, with a backend server, typically a database server. And I really mean 'as carefully as possible.' One new attack, called SQL poisoning, is designed to use a Web server to relay attacks against backend servers that run database software like Oracle or SQL Server. So, even if the data is not stored on the Web server itself, poor design of Web server scripts may leave the data still vulnerable to SQL poisoning attacks."

Hemorrhaging from theft of proprietary info?

In 1997, when we first asked questions about "types of attack" and "financial losses," 20% of respondents acknowledged detecting theft of proprietary information. In 2002, the percent of respondents acknowledging theft of proprietary information was the same. The high was in 2001, when 25% reported theft of proprietary information; the low was in 1998 when only 18% reported it.

But while the percent of respondents acknowledging theft of proprietary information has remained relatively steady, the total financial losses due to this type of activity among respondents willing and/or able to quantify their losses, as well as the average loss derived from the aggregate totals, has soared.

In 1997, 21 respondents quantified their losses. The highest reported loss was $10M, the average loss was $954,666, the total losses reported were $20,048,000. In 2002, 26 respondents quantified their losses. The highest reported loss was $50M, the average loss was $6,571,000, total losses reported were $170,827,000.

Why the significant increase in quantified financial losses due to theft of proprietary information when the percent of respondents reporting that type of activity has remained fairly constant?

Naomi Fine of Pro-Tec Data (www.pro-tecdata.com), a leading authority on economic espionage and information protection, explains.

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
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
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

2002: 321 Respondents/64%, 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
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
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

2002: 301 Respondents/60%, 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
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
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

2002: 289 Respondents/57%, 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 2002 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.

"The obvious answer is that those seeking information are more effective, perhaps because of more sophisticated technologies and techniques, at taking more valuable information. But the steady rise can also be attributed to two additional factors that have been rising exponentially over the same years as the study:

1) increased recognition that information has value.

2) increase in perceived value of information.

"In other words, while organizations like the Society for Competitive Intelligence Professionals help gatherers hone information collection skills, and the Internet makes it easier for information thieves to gather information used to bait and lure targets, the targets feel the pain of the loss more now because of an increased awareness that information translates into market differentiation, competitive positioning and even top line 'revenues.'"

Do you find the report of a $50 million loss due to theft of proprietary information implausible?

If you do, you simply don't read the business section of your newspaper closely enough.

In July 2001, Associated Press reported that Avant, a software company, was ordered to pay $182 million in restitution for stealing source code from Cadence, a competing firm, to settle one of Silicon Valley's longest running trade secret theft cases.

"Eight Avant company officials, including its chief executive, have pleaded no contest to felony trade secret theft charges. Cadence was seeking $700 million. The restitution was part of Santa Clara County's criminal case against Avant."

Fine elaborates on the substance behind such financial losses.

"In one case several years ago, involving Avery Dennison, one lost secret formula was quantified as being worth more than $40 million. In that case, Avery Dennison used only the cost of their investment. But if you add in lost profits or competitive advantage, trade secrets can be worth a lot more. Forgive me for being rhetorical, but if you were a large company, don't you think the loss of reputation alone due to a theft, say, of customer information entrusted to you would be worth more than $50 million?"

In its "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage for 2001," the Office of the National Counterintelligence Executive (NCIX) cited estimates of up to $100-$250 billion in lost sales for the previous year, with the most serious losses involving "information concerning manufacturing processes and research and development."

There were some high-profile cases in 2001.

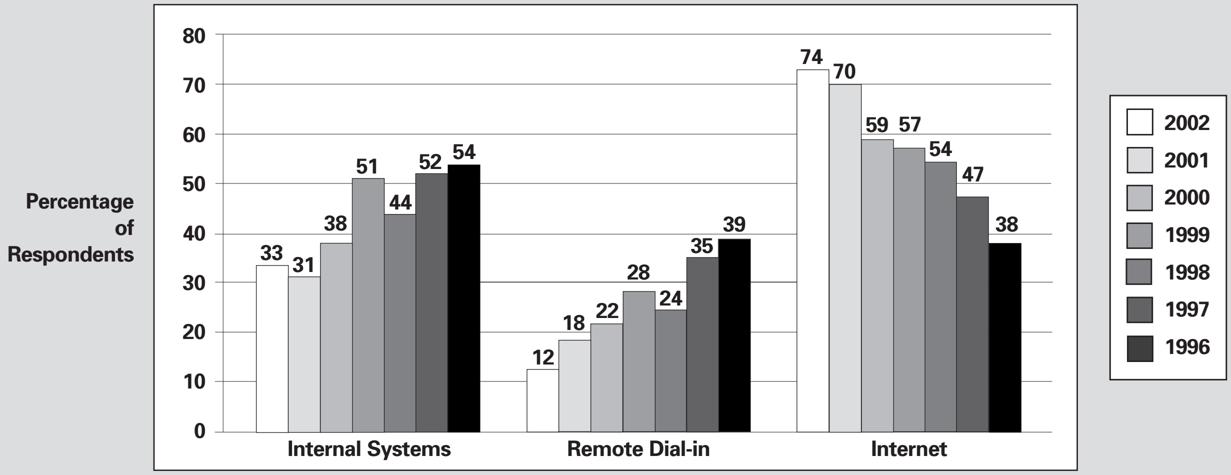
Two Chinese scientists and a U.S. citizen were arrested for stealing the source code to Lucent Technologies' PathStar for Beijing-based Datang Telecom.

Two Japanese medical researchers were arrested for stealing test tubes of genetic material from U.S. institutions for a brain research institute funded by the Japanese government.

The NCIX (www.ncix.gov) study cites "Internet activity (cyber attack and exploitation)" as one of the collection methods used by foreign corporations and governments in the conduct of economic espionage against U.S. targets.

"The majority of Internet endeavors are foreign probes searching for potential weaknesses in systems for exploitation. One example was

Internet Connection is Increasingly Cited as a Frequent Point of Attack



2002: 481 Respondents/96%
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 2002 Computer Crime and Security Survey
Source: Computer Security Institute

a network attack that, over the period of a day, involved several hundred attempts to use multiple passwords to illegally obtain access to a cleared defense facility's network. Fortunately, the facility had an appropriate level of protection in place to repel this attack. This example reflects the extent to which intelligence collectors are attempting to use the Internet to gain access to sensitive or proprietary information. Given the considerable effort that is under way in the cyber attack and exploitation arenas, substantial resources will need to be allocated in the future to ensure adequate security countermeasures."

But not every economic espionage case involved foreign spies or even high-tech, bio-tech or weapons secrets.

The U.S. DoJ's CCIP Web site displays a summary chart of cases prosecuted under the Economic Espionage Act (EEA) of 1986 (www.cybercrime.gov/eeapub.htm).

There you will find numerous cases involving trade secret theft engaged in by U.S. citizens and U.S. corporations domestically, as well as numerous cases involving unauthorized use of computer systems.

In December 2001, Mikahel K. Chang was sentenced to one year and one day in prison plus three years of supervised release for theft of trade secrets in U.S. District Court under the Economic Espionage Act. According to the plea agreement and his guilty plea, Chang, 33, of Santa Clara, CA confessed to "having received, possessed and, without authorization, appropriated stolen trade secret information" (i.e., sales databases) belonging to Chang's former employer, Semi Supply, Inc. of Livermore, CA, knowing that the information was "stolen, obtained and converted without authorization." Chang also admitted to having made $300,000 in gross sales using the Semi Supply databases, resulting in a $60,000 net profit for him.

Caryn Camp, a chemist at IDEXX Inc. (Portland, ME), a manufacturer of animal health test kits and other veterinary products, corresponded for seven months via e-mail with Dr. Stephen R. Martin, a California scientist.

In one e-mail message, Martin declared, "I never had a spy before. We are going to be in the veterinary business big time."

In the course of their on-line correspondence, Camp sent Martin some product and marketing information IDEXX considered confidential. When IDEXX became aware of the transfer, they reported Camp and Martin to the FBI.

Camp pleaded guilty to various criminal charges and agreed to testify against Martin. Martin was, in turn, convicted of multiple counts of conspiracy, EEA violations, mail and wire fraud, and interstate transportation of stolen property.

He lost his appeal and spent a year in prison.

Although cases documenting the hacking of trade secrets from the outside without insider knowledge are rarely made public, you would be very foolish indeed to think your organization's proprietary information was not at risk of attacks by professional hackers, whether acting for foreign governments or rival corporations.

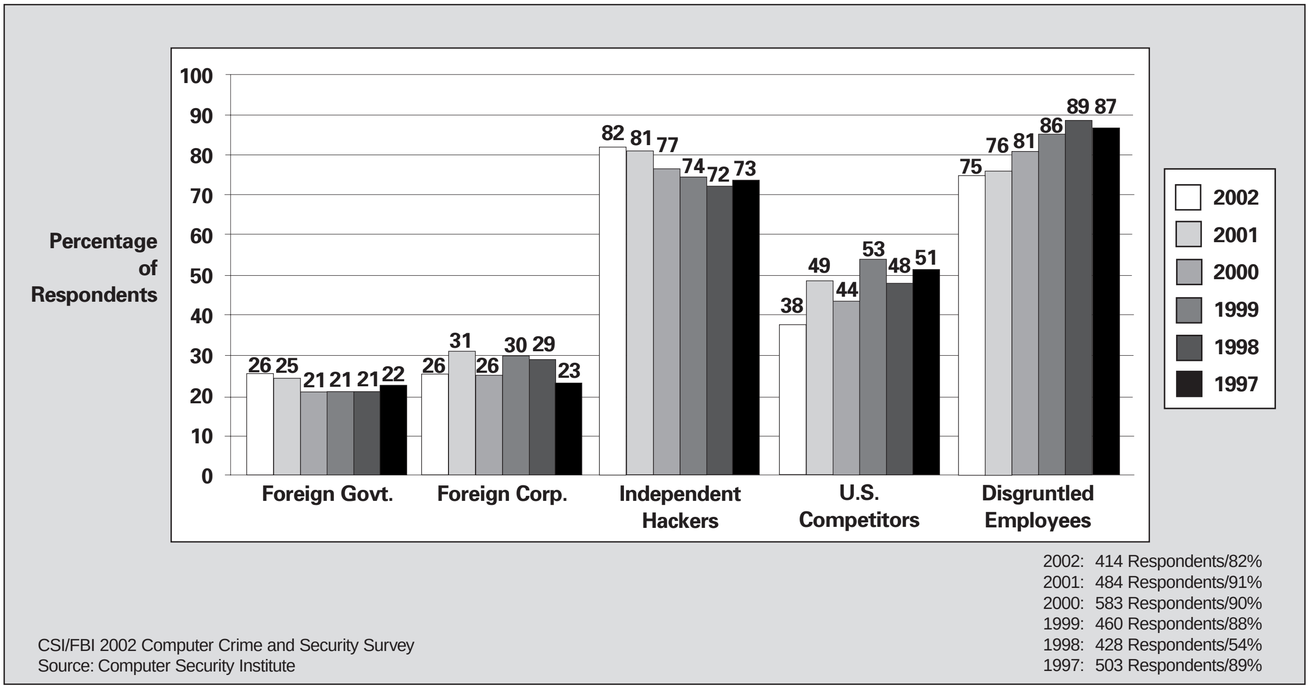
Another interesting trend in the data over the seven year life span of the survey is that the percent of respondents reporting U.S. domestic corporate competitors as a likely source of attack has gone either sideways or down: 51% in '97, 48% in '98, 53% in '99, 44% in '00, 49% in '01, 38% in '02. Perhaps the EEA, signed into law by President Clinton in 1996, really has had an impact.

Naomi Fine thinks so, but advises caution.

"I have seen a significant impact of the EEA on several fronts: 1) providing the statutory firepower to bring real justice to cases of high crimes that were previously stepchildren of the criminal justice system; 2) validating the perceived threat of information loss; 3) making companies aware of the benefits of taking reasonable measures to protect their own information; and 4) motivating companies to look at their own information gathering practices to determine their own potential liability.

"While I don't know what percentage of companies are compliant, my guess would be that most (well over 50%) of companies do not

Likely Sources of Attack



2002:	414 Respondents/82%
2001:	484 Respondents/91%
2000:	583 Respondents/90%
1999:	460 Respondents/88%
1998:	428 Respondents/54%
1997:	503 Respondents/89%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

engage in activities that violate the EEA, whereas most (well over 50%) of companies do not have a formal compliance program in place. I would translate this to mean that the risk is high that employees of many companies and many companies themselves will at some time or another violate the EEA because they don't have the infrastructure of a compliance program to counter the temptation to take information in violation of the EEA."

Hemorrhaging from financial fraud?

Like theft of proprietary information, financial fraud accounts for a disproportionate amount of the aggregate financial losses cited by those willing and/or able to quantity. And also like theft of proprietary information, while the losses attributed to financial fraud have increased significantly, the percent of those respondents acknowledging detection of financial fraud has remained fairly constant.

In 1997, when we first asked questions about "types of attack" and "financial losses," 12% of respondents acknowledged detecting financial fraud. In 2002, the percent of respondents acknowledging financial fraud was the same. The high was 14% in 1998 and 1999, when 14% reported financial fraud; the low was in 2000 when only 11% reported it.

But while the percent of respondents acknowledging financial fraud has remained relatively steady, the total financial losses due to this type of activity among respondents willing and/or able to quantify their losses, as well as the average loss derived from the aggregate totals, has soared.

In 1997, 26 respondents quantified their losses. The highest reported loss was $2 million, the average loss was $957,384 the total losses reported were $24,892,000. In 2002, 25 respondents quantified their losses. The highest reported loss was $50M, the average loss was $4,632,000, and total losses reported were $115,753,000.

In October 2001, Vasiliy Gorshkov, age 26, of Chelyabinsk, Russia, was found guilty on 20 counts of conspiracy, various computer crimes, and fraud committed against Speakeasy Network (Seattle, WA) Nara Bank (Los Angeles, CA), Central National Bank (Waco, TX), and PayPal (Palo Alto, CA), an online credit card payment company.

Gorshkov and another man, Alexey Ivanov, were lured from Chelyabinsk to Seattle in an FBI undercover operation.

The DoJ's Computer Crime and Intellectual Property (CCIP) Web site (www.usdoj.gov/criminal/cybercrime/cccases.html) provides some details.

"The operation arose out of a nationwide FBI investigation into Russian computer intrusions that were directed at Internet Service Providers, e-commerce sites, and online banks in the United States. The hackers used their unauthorized access to the victims' computers to steal credit card information and other personal financial information, and then often tried to extort money from the victims with threats to expose the sensitive data to the public or damage the victims' computers. The hackers also defrauded PayPal through a scheme in which stolen credit cards were used to generate cash and to pay for computer parts purchased from vendors in the United States.

"A few days after the two men were arrested, the FBI obtained access via the Internet to two of the men's computers in Russia. The FBI copied voluminous data from the accounts of Gorshkov and Ivanov. The data copied from the Russian computers provided a wealth of evidence of the men's computer hacking and fraud. They had large databases of credit card information that was stolen from Internet Service Providers. More than 56,000 credit cards were found on the two Russian computers. The Russian computers also contained stolen bank account and other personal financial information of customers of online banking at Nara Bank and Central National Bank in Waco.

"The data from the Russian computers revealed that the conspirators had gained unauthorized control over numerous computers–including computers of a school district in St. Clair County, MI–and then used those compromised computers to commit

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 72-month period.

How money was lost

	Respondents w/ Quantified Losses						Lowest Reported						Highest Reported					
	'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02
Theft of proprietary info.	21	20	23	22	34	26	$1K	$300	$1K	$1K	$100	$1K	$10M	$25M	$25M	$25M	$50M	50M
Sabotage of data of networks	14	25	27	28	26	28	$150	$400	$1K	$1K	$100	$1K	$1M	$500K	$1M	$15M	$3M	10M
Telecom eavesdropping	8	10	10	15	16	5	$1K	$1K	$1K	$200	$1K	$5K	$100K	$200K	$300K	$500K	$500K	5M
System penetration by outsider	22	19	28	29	42	59	$200	$500	$1K	$1K	$100	$1K	$1.5M	$500K	$500K	$5M	$10M	5M
Insider abuse of Net access	55	67	81	91	98	89	$100	$500	$1K	$240	$100	$1K	$100K	$1M	$3M	$15M	$10M	10M
Financial fraud	26	29	27	34	21	25	$5K	$1K	$10K	$500	$500	$1K	$2M	$2M	$20M	$21M	$40M	50M
Denial of service	n/a	36	28	46	35	62	n/a	$200	$1K	$1K	$100	$1K	n/a	$1M	$1M	$5M	$2M	50M
Spoofing	4	n/a	n/a	n/a	n/a	n/a	$1K	n/a	n/a	n/a	n/a	n/a	$500K	n/a	n/a	n/a	n/a	n/a
Virus	165	143	116	162	186	178	$100	$50	$1K	$100	$100	$1K	$500K	$2M	$1M	$10M	$20M	9M
Unauthorized insider access	22	18	25	20	22	15	$100	$1K	$1K	$1K	$1K	$2K	$1.2M	$50M	$1M	$20M	$5M	1.5M
Telecom fraud	35	32	29	19	18	16	$300	$500	$1K	$1K	$500	$1K	$12M	$15M	$100K	$3M	$8M	100K
Active wiretapping	n/a	5	1	1	0	0	n/a	$30K	$20K	$5M	$0	$0	n/a	$100K	$20K	$5M	$0	0
Laptop theft	165	162	150	174	143	134	$1K	$1K	$1K	$500	$!K	$1K	$1M	$500K	$1M	$1.2M	$2M	5M

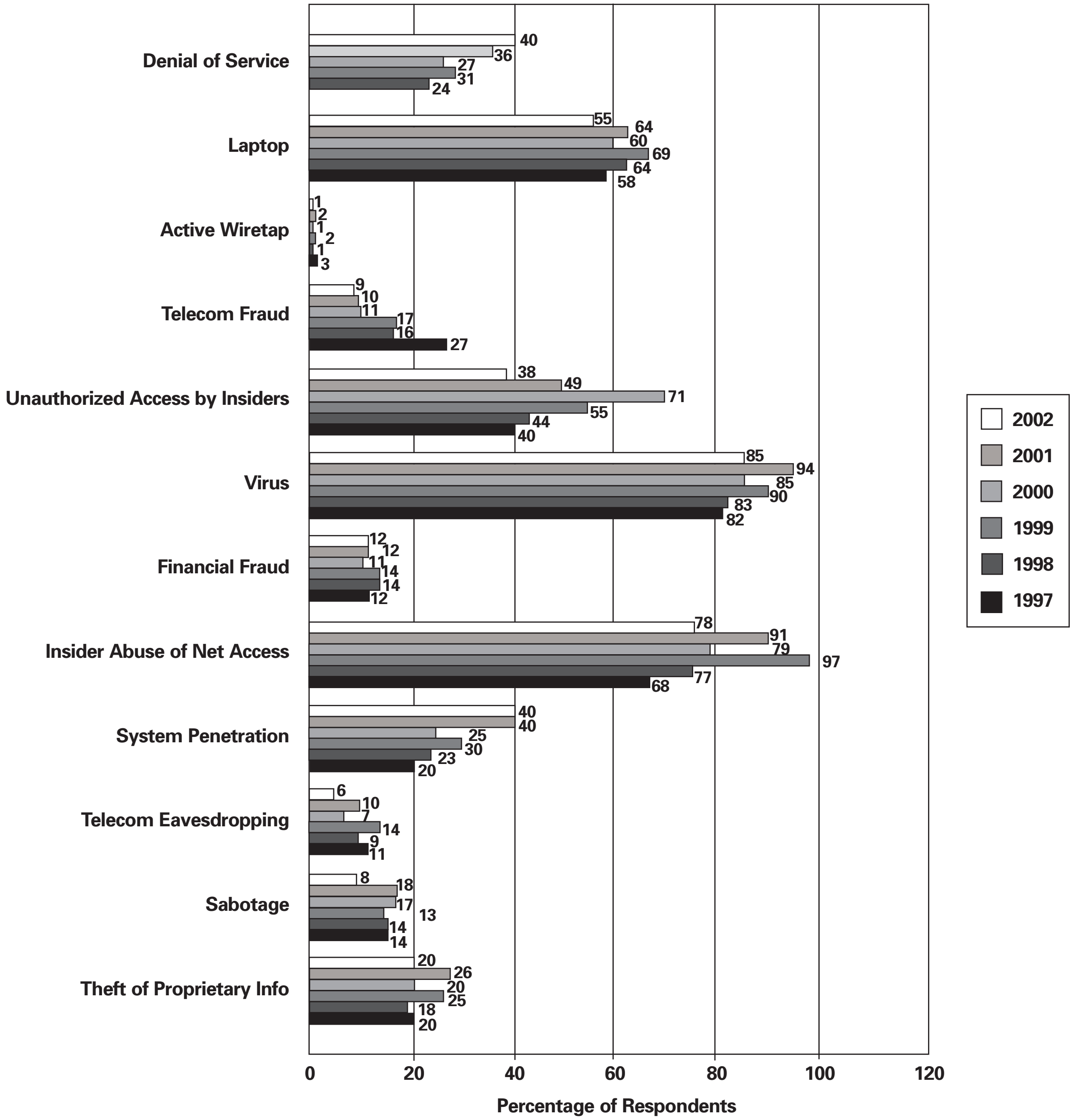
CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Note: In 2002, 80% of our survey respondents acknowledged financial losses, but only 44% of respondents could quantify the losses.

Average Losses						Total Annual Losses					
'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02
$954,666	$1,677,000	$1,847,652	$3,032,818	$4,447,900	$6,571,000	$20,048,000	$33,545,000	$42,496,000	$66,708,000	$151,230,100	$170,827,000
$164K	$86K	$163,740	$969,577	$199,350	$541,000	$4,285,850	$2,142,000	$4,421,000	$27,148,000	$5,183,100	$15,134,000
$45,423	$56K	$76,500	$66,080	$55,375	$1,205,000	$1,181,000	$562,000	$765,000	$991,200	$886,000	$6,015,000
$132,250	$86K	$103,142	$244,965	$453,967	$226,000	$2,911,700	$1,637,000	$2,885,000	$7,104,000	$19,066,600	$13,055,000
$18,304	$56K	$93,530	$307,524	$357,160	$536,000	$1,006,750	$3,720,000	$7,576,000	$27,984,740	$35,001,650	$50,099,000
$957,384	$388K	$1,470,592	$1,646,941	$4,420,738	$4,632,000	$24,892,000	$11,239,000	$39,706,000	$55,996,000	$92,935,500	$115,753,000
n/a	$77K	$116,250	$108,717	$122,389	$297,000	n/a	$2,787,000	$3,255,000	$8,247,500	$4,283,600	$18,370,500
$128K	n/a	n/a	n/a	n/a	n/a	$512,000	n/a	n/a	n/a	n/a	n/a
$75,746	$55K	$45,465	$180,092	$243,845	$283,000	$12,498,150	$7,874,000	$5,274,000	$29,171,700	$45,288,150	$49,979,000
$181,437	$2,809,000	$142,680	$1,124,725	$275,636	$300,000	$3,991,605	$50,565,000	$3,567,000	$22,554,500	$6,064,000	$4,503,000
$647,437	$539K	$26,655	$212,000	$502,278	$22,000	$22,660,300	$17,256,000	$773,000	$4,028,000	$9,041,000	$346,000
n/a	$49K	$20K	$5M	$0	$0	n/a	$245,000	$20,000	$5,000,000	$0	$0
$38,326	$32K	$86,920	$58,794	$61,881	$89,000	$6,132,200	$5,250,000	$13,038,000	$10,404,300	$8,849,000	$11,766,500
					Total Annual Losses:	$100,119,555	$136,822,000	$123,799,000	$265,337,990	$377,828,700	$455,848,000

Grand total of Losses reported (1997-2001): $1,459,755,245

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



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

2002: 455 Respondents/90%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/83%
1997: 503 Respondents/89%

a massive fraud involving PayPal and the online auction company e-Bay. The fraud scheme consisted of using computer programs to establish thousands of anonymous e-mail accounts at e-mail web sites like Hotmail, Yahoo!, and MyOwnEmail.

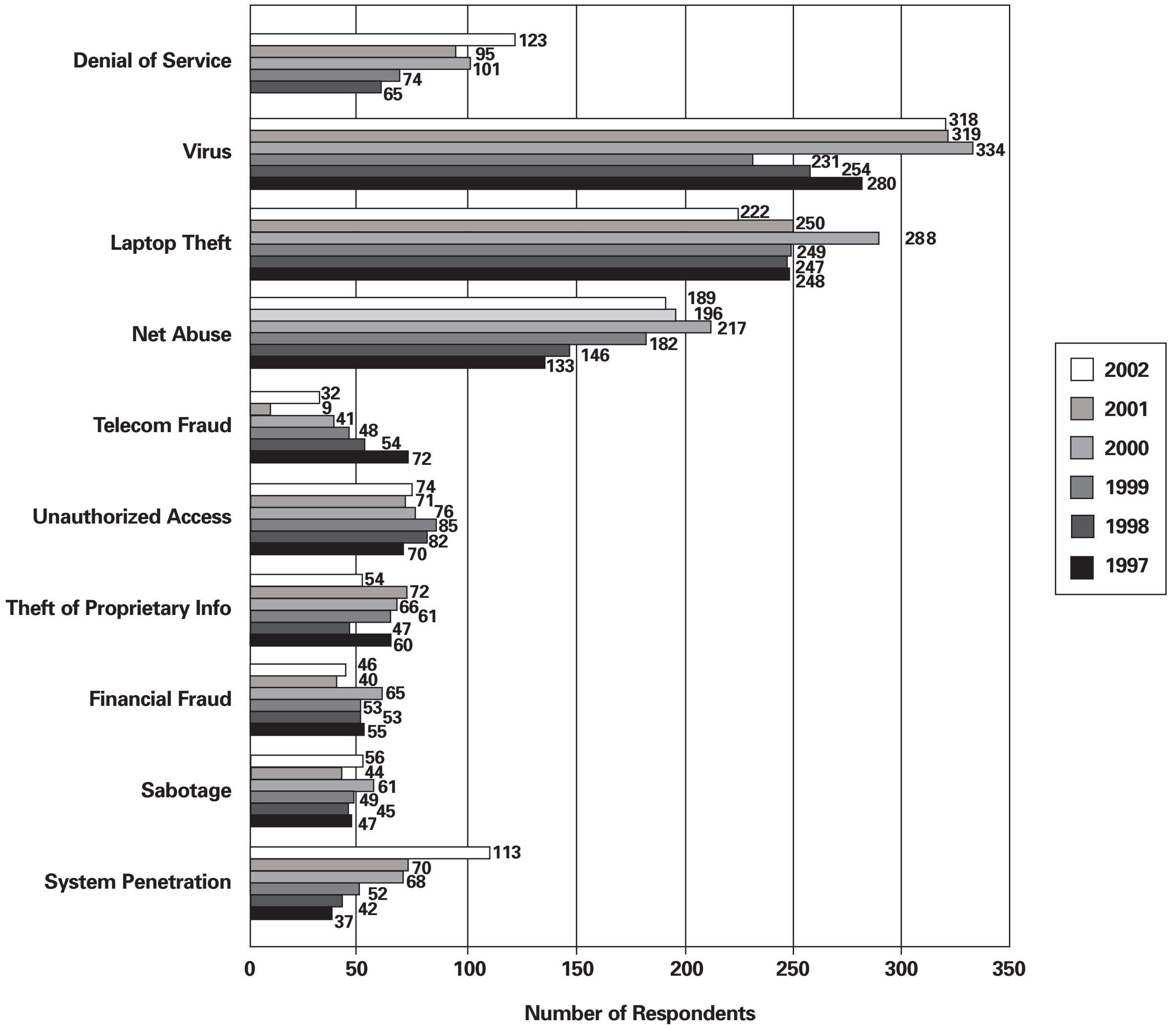
"Gorshkov's programs then created associated accounts at PayPal with random identities and stolen credit cards. Additional computer programs allowed the conspirators to control and manipulate e-Bay auctions so that they could act as both seller and winning bidder in the same auction and then effectively pay themselves with stolen credit cards."

The Gorshkov case is not an isolated incident. It provides a glimpse into the growing digital underworld that has emerged in the ruins of the former Soviet Union.

In January, 2002, the *Computer Business Review* reported that a Russian computer hacker had been detained on suspicion of extorting $10,000 from a US bank after breaking into its database and threatening to publish account details.

"The suspect, identified only as Nikolai, was detained in the western Siberian town of Surgut after Moscow police's computer fraud unit was approached by the U.S. embassy.

Financial Losses by Type of Attack or Misuse



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

2002: 404 Respondents/80%
2001: 344 respondents/64%
2000: 477 Respondents/74%
1999: 376 Respondents/73%
1998: 512 Respondents/98%
1997: 422 Respondents/75%

"According to reports in the Russian press, Nikolai broke into the Web server of Online Resources Corp., a McLean, VA company, that offers Internet banking, bill payment and e-finance application services to financial institutions. Nikolai, a 21-year-old university drop-out, then attempted to extort money from an unnamed New York bank by threatening to publish account details. To buttress the threat, he posted details from 1,500 accounts online. The bank paid out $10,000 in December but estimates its total financial damage at $250,000. The Moscow computer fraud unit managed to track him by his IP address when he exchanged e-mail addresses with the bank, and he is now in custody facing 15 years jail."

Of course, the growing number of incidents of theft of proprietary information and financial fraud from the outside has only added to the woes of information security professionals in Fortune 500 corporations and large government agencies. However, the insider threat is still very real and very costly.

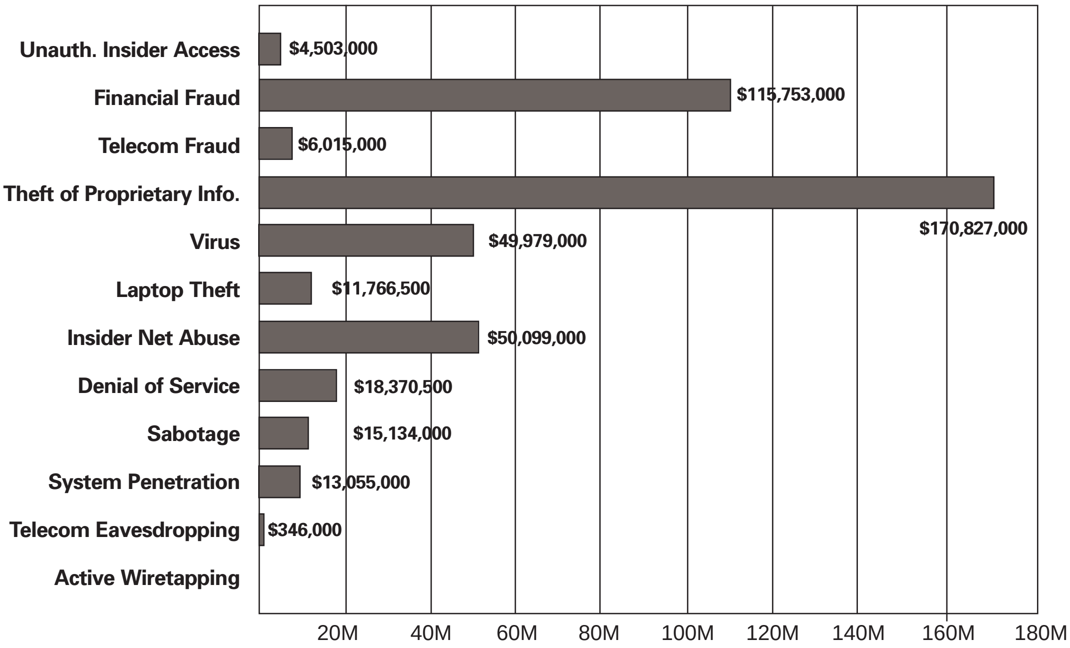
Consider two recent cases.

In November 2001, two former Cisco Systems, Inc., accountants Geoffrey Osowski and Wilson Tang were sentenced to 34 months in prison for "exceeding their authorized access to the computer systems" of Cisco Systems in order to illegally issue almost $8 million in Cisco stock to themselves.

The DoJ CCIP Web site provides some details.

"In pleading guilty, Osowski and Tang admitted that between October 2000 and March 27, 2001, they participated together in a scheme to defraud Cisco Systems in order to obtain Cisco stock that they were not authorized to obtain. As part of the scheme, they exceeded their authorized access to computer systems at Cisco in order to access a computer system used by the company to manage stock option disbursals, used that access to identify control numbers to track authorized stock option disbursals, created forged forms purporting to authorize disbursals of stock, faxed the forged requests to the company

Dollar Amount of Losses by Type



CSI/FBI 2002 Computer Crime and Security Survey
Sourxe: Computer Security Institute

2002: 223 respondents/44%

responsible for controlling and issuing shares of Cisco Systems stock, and directed that stock be placed in their personal brokerage accounts.

The two defendants admitted that the first time that they did this, in December 2000, they caused 97,750 shares of Cisco stock to be placed in two separate Merrill Lynch accounts, with 58,250 of the shares deposited in an account set up by Osowski and 39,500 shares deposited in an account set up by Tang. In February 2001, they caused two additional transfers of stock, in amounts of 67,500 shares and 65,300 shares, to be transferred to brokerage accounts in their names. The total value of the Cisco stock that they took on these three occasions (at the time that they transferred the stock) was approximately $7,868,637.

In March 2002, U.S. federal agents working with the New York Electronic Crimes Task Force arrested Donald Matthew McNeese on charges of identity theft, credit card fraud and money laundering after he stole a computer database containing personnel records for as many as 60,000 employees of the Prudential Insurance Co. and attempted to sell the data over the Internet.

McNeese had worked as the administrator of the database at Prudential's Jacksonville, Florida office until June 2000.

The federal complaint states that McNeese not only offered to sell Prudential employees' identities over the Internet, but was also engaged in other activity related to credit card fraud.

Again, the DoJ CCIP Web site provides some details.

"For example, using e-mail screen names that were stolen from his victims, he attempted to advise other readers at an online newsgroup about various aspects of credit card fraud. For the use of those newsgroup readers, McNeese posted personal information for, and credit card numbers belonging to, Prudential employees so that the readers could use the information to obtain fraudulent credit cards in the employees' names. He also sought online advice about engaging in a scheme to obtain money from fraudulent credit cards through money-remitting businesses. Finally, the government alleges that McNeese sent e-mails to the victims of his credit card fraud scheme, falsely incriminating his former boss as the perpetrator of the fraud."

Rebecca Herold, Senior Security Architect of QinetiQ Trusted Information Management, Inc. (http://qinetiq-tim.com/), sheds some light on the problem of computer-based financial fraud and why the losses attributed to it have increased dramatically over the life of the survey.

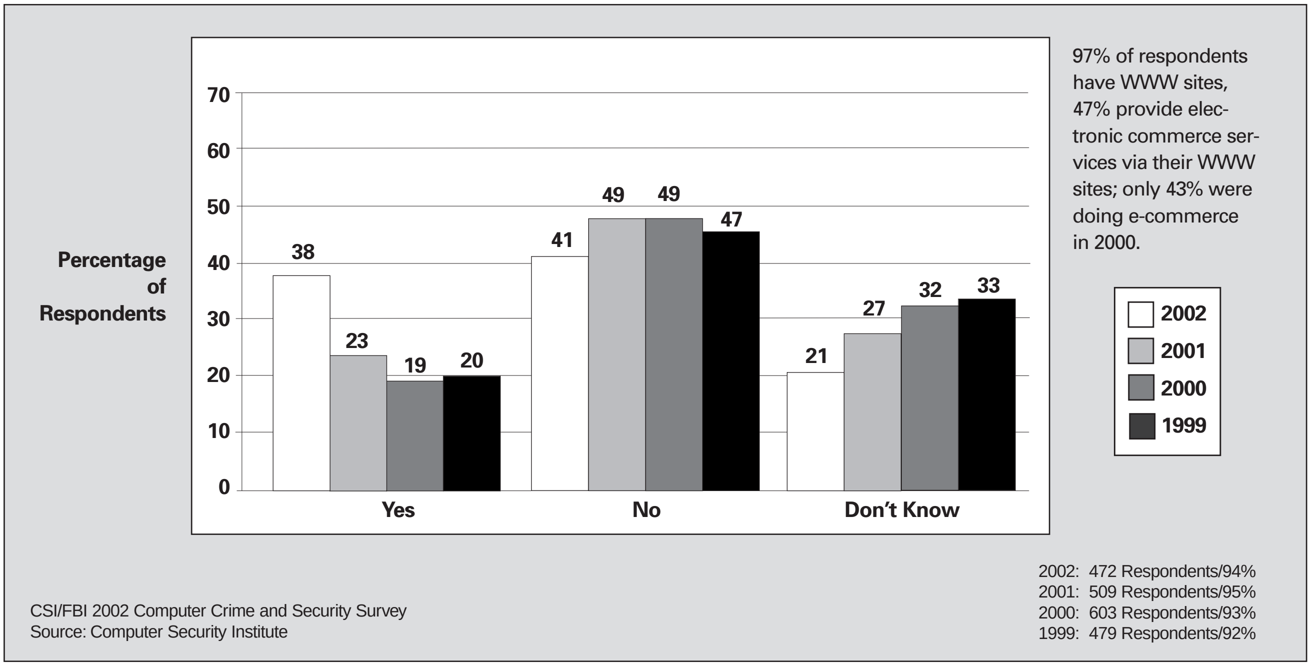
"The amount of financial transactions occurring electronically has grown exponentially over the past decade. As organizations race to create e-commerce systems so they do not miss the perceived bandwagon, they often create applications that have poor and, sadly, often no security built into the systems architecture and procedural controls. Or they contract the creation of such e-commerce systems to organizations who have no experience in building security into architectures and may omit security controls altogether. Additionally, the amount of technical savvy of organizational staff has increased steadily over the years. Unscrupulous employees and personnel who recognize an organization's network and procedural control weaknesses will take the opportunity to exploit those weaknesses in fraudulent ways resulting in potentially huge financial losses to the organizations.

"Sadly, security controls and tools are often the victims of budget cuts when project costs must be reduced when implementing new applications, systems or networks. I've heard too many organizations say that they will add security 'later' after implementation so they can meet their target dates, and then later never comes. What this results in is lack of security and procedural controls, and poor or non-existent audit trails, that could be used to identify attempted financial fraud before it occurs.

"In addition to poorly constructed security and substandard audit trails, there are also inadequate or nonexistent procedures for removing access to systems and information following personnel dismissal or loss of customers as a result of dissatisfaction.

"Finding published examples of financial fraud incidents is often

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.

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

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

difficult. Most organizations do not make financial fraud incidents public because they do not want the bad PR, and they do not want federal law enforcement getting involved. It's often perceived as easier for the companies to take the loss and put a bandage solution on the weakness that allowed the fraud to begin with. So, when organizational leaders do not see such cases in their Wall Street Journals and other publications, they assume such activity is not occurring.

"However, of the press releases that exist, most involve employees, former employees and/or unauthorized remote access, and all could have arguably been prevented had good security and audit procedures and controls been in place.

"It is interesting, that while financial fraud values continue a rocketing rise within the business sector, during the same time the occurrence of identity theft has also risen at alarming rates for private citizens. In fact, identity theft accounted for 42 percent of the 204,000 complaints entered into the FTC's Consumer Sentinel database last year. These numbers should demonstrate to company management that financial fraud is not something that is just happening to some other unlucky companies, or within industries other than their own. Financial fraud is being attempted anywhere the perpetrators see an opportunity.

"As the world becomes more electronically connected and integrated, attempts at committing financial fraud are not going to lessen…they are only going to increase and do so dramatically in all public and private sectors unless security is taken seriously and addressed. Leaders need to recognize that they must invest in integrating security within all aspects of their business systems and procedural controls. They cannot in good faith gamble on their organizations not being a target of financial fraud attempts because they perceive there are bigger, more appealing targets out there. The cost of implementing security must be considered a cost of doing business. Leaders cannot depend upon security by obscurity, or more bluntly, ignorance, as a control. Don't underestimate personnel, unauthorized systems users or anyone else who has access not to compromise or take advantage of your procedural or system weaknesses. It only takes one incident to cost your company millions of dollars more than it would have to incorporate security from the very beginning. Can you afford to stay in business following one multi-million dollar fraud?"

Other Serious Problems: Viruses, Worms, etc.

Theft of proprietary information and financial fraud account for perhaps two-thirds of the financial losses reported by respondents. Yet only 20% report incidents of theft of proprietary information, and only 12% report incidents of financial fraud.

Furthermore, throughout the seven-year life of the survey, these ratios have held fairly steady.

So what does the rest of the story tell us? What types of attacks or breaches are the most common? And what kind of financial losses do they incur?

It will probably be no surprise to you that malicious code attacks (i.e., viruses, worms, etc.) have proven year in and year out to be the most common incidents reported in the survey.

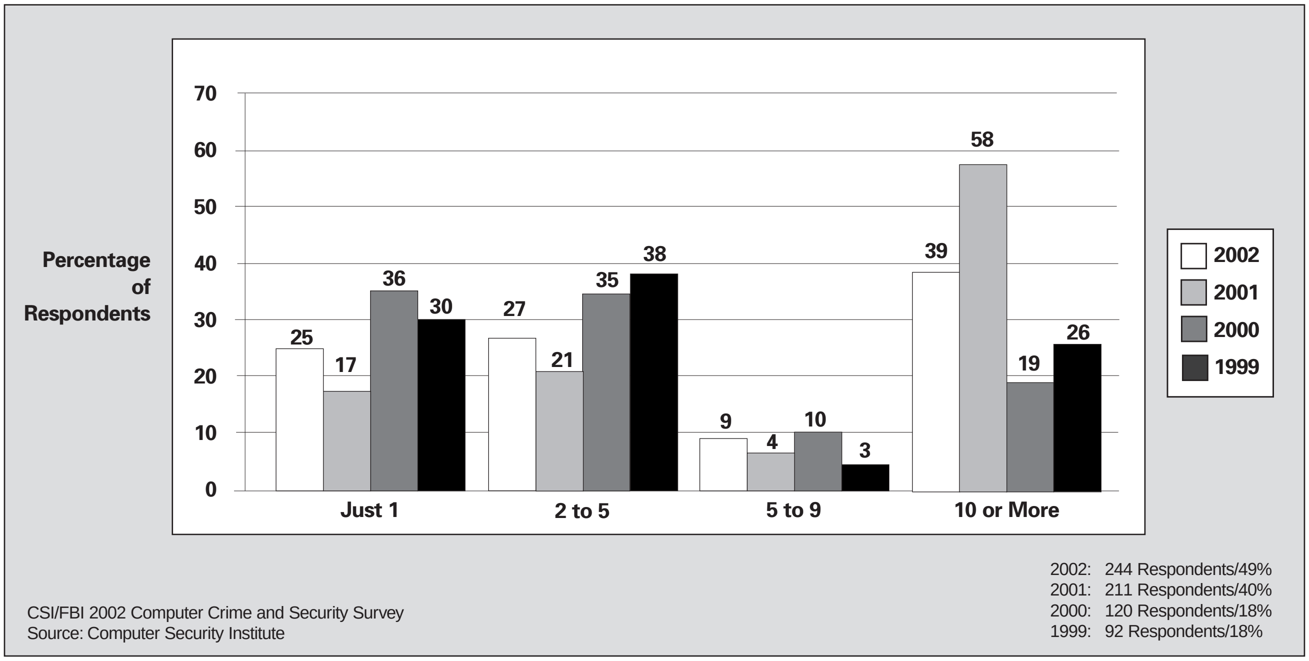
In 1997, 82% of respondents reported virus and worm contaminations. In 2001, the year in which the survey results reflected those hit by "I Love You," the percent of respondents reporting viruses, etc. peaked at 94%.

In 1997, financial losses due to viruses, etc. were reported by 165 respondents for an aggregate total of $12,498,150 with an average of loss of $75,746 per organization.

In 2001, financial losses due to viruses, etc. were reported by 186 respondents for an aggregate total of $45,288,150 with an average loss of $243,845 per organization.

In 2002, although the percent of respondents reporting virus and worm outbreaks dropped from 94% the previous year to 85%, the total financial losses reported by the 188 respondents who were willing/and or able to quantify actually increased from

WWW Site Incidents: If Yes, How Many Incidents?



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

$45,288,600 to $49,979,000 with an increase in the average loss from $243,845 per organization in 2001 to $283,000 per organization in 2002.

While the 2001 results reflect the impact of "I Love You," the 2002 results would reflect those respondents hit by CodeRed, Nimda and Sircam.

Computer Economics (www.computereconomics.com) estimates that the worldwide economic impact of Code Red was $2.62 billion, the worldwide economic impact of SirCam was $1.15 billion and the world economic impact of Nimda was $635 million. Computer Economics further estimates the worldwide economic impact of "I Love You" in 2000 at $8.75 billion and that of Melissa and Explorer in 1999 at $1.10 billion and $1.02 billion respectively.

The total financial losses that respondents (500 or so organizations, mostly major corporations and large government agencies, over a seven year period) were willing and/or able to quantify in the CSI/FBI survey from1997 until 2002, including CodeRed, SirCam, Nimda, "I Love You," Melissa, and Explorer as well as numerous others to a far lesser extent adds up to $150,085,000.

I leave you to draw your own conclusions.

Other Serious Problems: Net Abuse, etc.

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) dropped from 91% in 2001 to 78% in 2002, and yet, financial losses attributed to this type of abuse, etc. soared from $35,001,650 with an average loss per organization of $357,160 in 2001 to $50,099,000 with an average of $536,000 in 2002. How and why?

Organizations are more sensitive to the costs of the problem. They are watching their workforce more closely. They are more in control of what is going on. They are getting tougher. They are making examples of people. The Internet filtering and monitoring technology they have invested in is paying off.

High-profile crackdowns on Net abuse at Dow Chemical Co., the *New York Times*, Computer Associates International, First Union Corp., Edward Jones, Livermore National Lab and numerous U.S. government agencies have whetted the appetite of other organizations.

Organizations are taking the problem seriously.

According to the American Management Association, seventy-three percent of U.S. businesses monitored their employees' Internet use last year.

Organizations are cracking down harder than ever.

Websense, an Internet filtering provider, reports that nearly two-thirds of U.S. companies disciplined workers for misusing Internet privileges while working, and a third of them–ranging in size from 6 to over 150,000 employees–have terminated workers that use the Internet to loaf.

Organizations are spending lots of money on it.

International Data Corp. forecasts that the Internet filtering technology market will grow by close to 50% per year, reaching $636 million (707.8 million euros) worldwide by 2004.

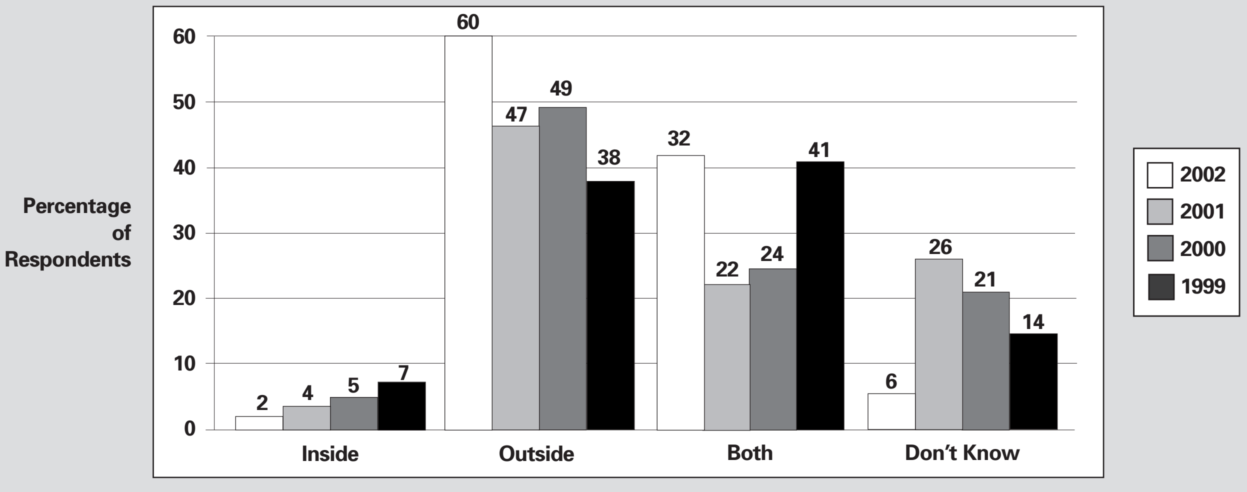
And the well-funded crackdown is world-wide.

The Privacy Foundation estimates that the number of employees under such surveillance is at 27 million, just over one-quarter of the global online workforce, i.e., those employees who have Internet and/or e-mail access at work, and use it regularly.

The problem isn't simply insiders accessing pornographic sexual content.

For example, the Informa Media Group projects that e-gambling revenue will rise to $14.5 billion worldwide by 2006. Informa believes that by that time, the U.S. will claim 24% of e-gambling revenue, and Europe will claim 53%. The Society for

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



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

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

Human Resource Management reports that 30 percent of employees dive into NCAA office gambling pools. According to PC Data Online, approximately 14 million people visited sports Web sites during last year's NCAA college basketball tournament, aka “March Madness.” Websense estimates organizations could suffer $504 million in lost productivity due to employees checking scores and viewing game Webcasts during work hours.

For corporations and government agencies, net abuse is a problem that effects the bottom line.

The issue isn't morality. The issue is productivity. Whether they are shopping on-line or surfing for film clips of kinky sex, workers get less done if they succumb to the many temptations of the Web.

The issue isn't censorship. The issue is civil liability. What is humorous or sexually arousing to one person is often threatening or offensive to another person. A successfully waged sexual harassment law suit can results in hundreds of thousands or even millions of dollars in damages.

Nor are the 103 organizations that were willing and/or able to quantify the aggregate financial losses of $50,099,000 just tabulating the impact of time spent shopping, fantasizing or gambling on-line, other egregious abuse of Internet and network privileges are reflected in that $50 million plus figure. Financial losses due to incidents of inappropriate e-mail usage and software piracy also factor into the equation.

Software piracy in the workplace?

In November 2001, Software and Information Industry Alliance (SIIA), formerly known as the SPA, and KPMG LLP reported that of the 1,004 business people they surveyed, more than half of the business users said they were unaware of corporate policies governing intellectual property that may be in place.

According to the study, 54 percent of business users indicated they do not know if it is permissible to redistribute information from on-line sites they subscribe to, while 23 percent said they believe it is permitted.

The survey, conducted to examine the acquisition and use of software and digital content via the Internet, found that nearly 30% of business people could be classified as pirating software through a variety of electronic methods.

Inappropriate e-mail usage?

Consider this BBC story.

“Peter Chung, an investment banker, took a job with equity investment firm The Carlyle Group in Seoul. Not long after his arrival he sent an e-mail to his former colleagues detailing his intentions to bed as many local women as possible and to indulge himself in free entertainment from bankers hoping to do business with the company.

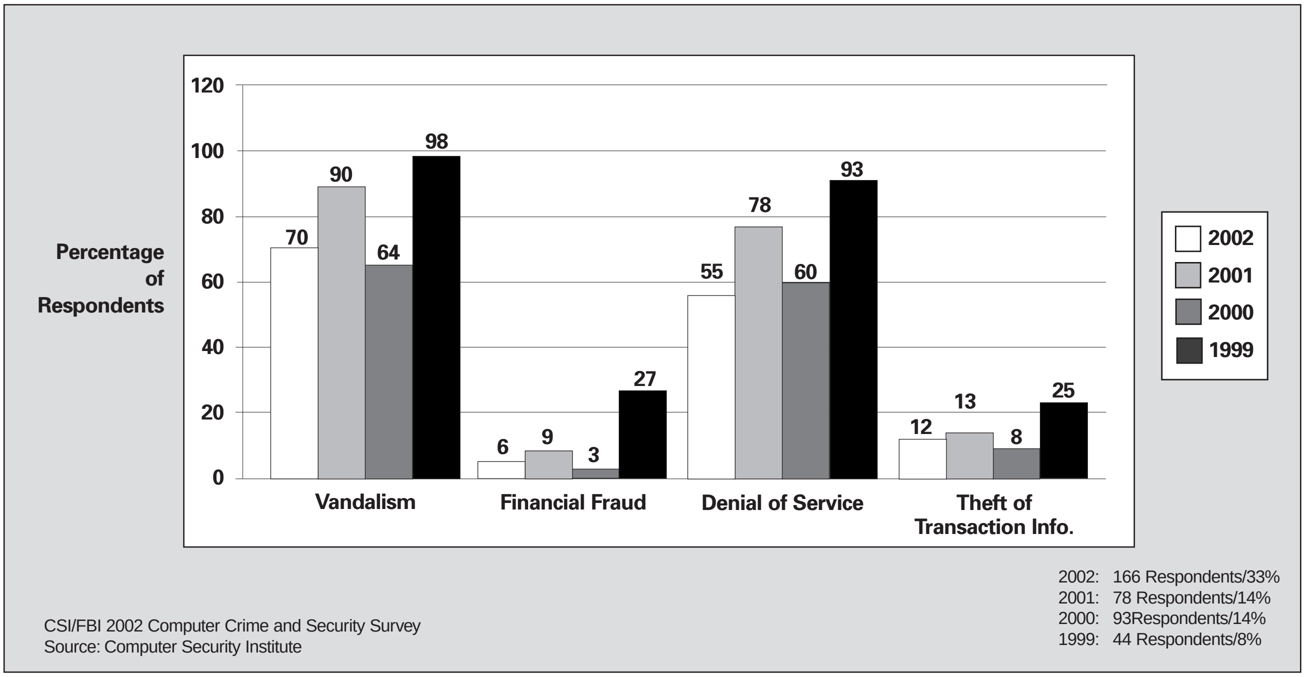
“The e-mail was forwarded to friends, who in turn forwarded it to more friends. Soon his e-mail had circled the globe and been posted on the internet. The Carlyle Group's management was apparently not amused, and Chung resigned shortly afterwards in disgrace.”

Post-9/11 gut check

As time spreads out and days, weeks and months distance us from the flashpoint of 9/11, many new challenges in regard to how we deal with security in our lives and our work have to be met. Well, most of them are not really new challenges. It is simply that we have woken up to them at last. Admittedly, in an environment in which the availability of smallpox vaccine and the potential impact of a jetliner crashing into a nuclear reactor have to be factored in, it is difficult to see the range of cyber threats–whether a nuisance virus or an infrastructure attack–as a serious issue. And yet, there are few (other than weapons of mass destruction) that are more urgent.

Remembering, as I am sure you do, the psychological toll of live TV coverage of jetliners being piloted into the twin towers of the World Trade Center, remembering, as I am sure you do, the ghastly horror of what followed as the giant structures collapsed suddenly and utterly ending thousands of lives—imagine what the psychological impact would have been if those images had been the last ones you saw on your TV screen because of an infrastructure attack on the telecommunications network.

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



2002: 166 Respondents/33%
2001: 78 Respondents/14%
2000: 93Respondents/14%
1999: 44 Respondents/8%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

Remembering, as I am sure you do, the terrorist attack's severe impact on the transportation industry and other vital sectors of the U.S. economy, imagine if those astounding acts of physical violence had been followed by a series of infrastructure attacks on the air traffic control system, the power grid or the financial markets.

The economic and psychological toll of such infrastructure attacks could be serious and if (or when) combined with physical attacks against the populace they could be devastating.

Where does that leave you and your organization? What is your role? What do you need to do?

Some 9/11 lessons have stuck with me.

Information security does not exist in isolation.

You cannot secure your information or the systems that it flows through and is stored on unless you also pay attention to other aspects of the overall security posture of your organization–for example, personnel security, physical security and home security.

And conversely, you cannot secure your organization's physical perimeter or your organization's workforce unless you have also secured your organization's information systems to the best of your ability (or that of those with the requisite expertise and resources that you have contracted with outside of your organization).

What does the world look like after 9/11? What it looked like before 9/11. It is just that we see it better and hopefully understand it more.

Your organization needs to commit itself to information security with appropriate organizational clout (i.e. an information security team reporting directly to the CIO or better), adequate staffing levels (most organizations still have only one information security professional for every thousand users), adequate budget dollars (despite a lot of talk, most organizations don't spend more than 1-3% or 3-5% of their total IT budget on security), adequate training for technicians and users alike (your organization can be bristling with firewalls and IDS, but if a naive user ushers an attacker in through the back door you have wasted your money).

If you have not, or will not, attended to these vital areas of an information security program, you are throwing your money away on whatever sophisticated technology you purchase and deploy.

If you attend to the issues of training, staffing, budgeting, and organizational clout, as well as bulking up with the latest proven technologies, you will significantly mitigate your levels of risk to a wide range of unfortunate events.

Remember that during economic downturns, insiders (i.e. employees, ex-employees, contractors, ex-contractors, etc.) are under even greater pressure to commit fraud, theft of proprietary information or sabotage on your networks. Remember, too, that during times of national emergency and international crisis, criminal elements will take advantage of the fact that law enforcement at all levels (state, local and federal) are focused elsewhere and seize the moment to rape your servers and plunder your secrets.

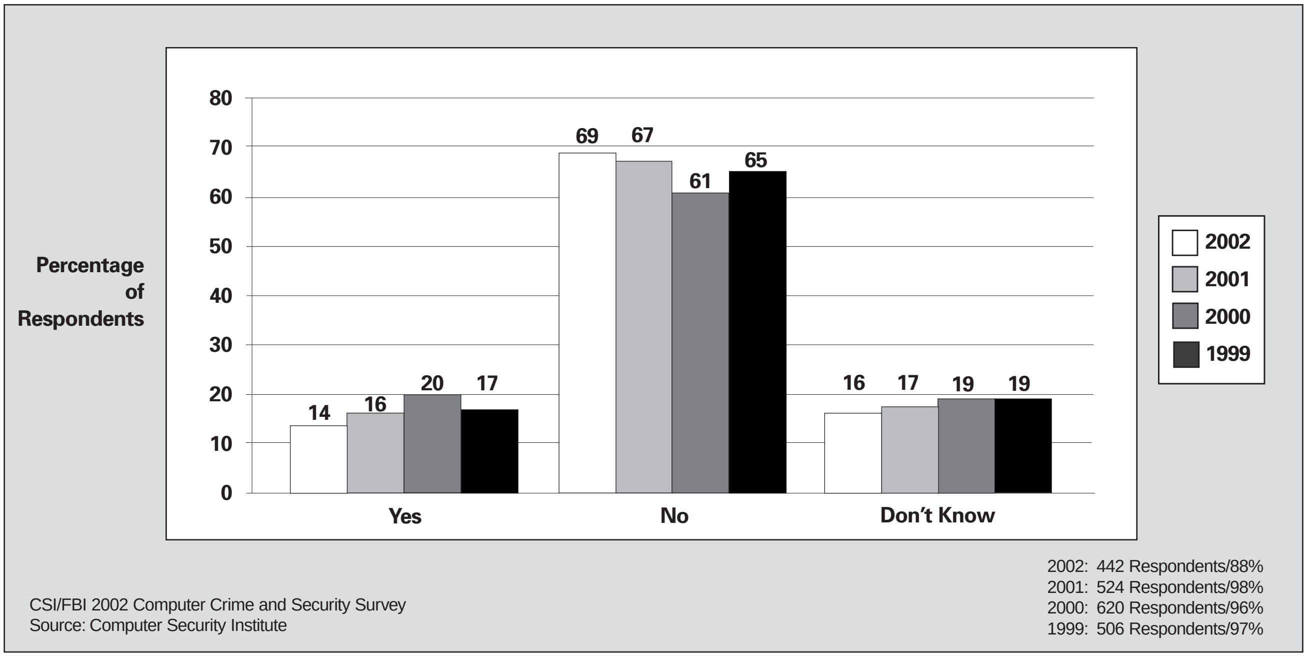
Here are a few important items to consider, discuss and hopefully act on within your organization.

First, update and upgrade your disaster recovery and business continuity plans.

If your organization already has disaster recovery and business continuity plans, have you reviewed them in the aftermath of 9/11? If your organization does not already have disaster recovery and business continutity plans, do you know where to begin? A comprehensive list of recommendations for disaster recovery and business continuity planning (whichever position you find yourself in) can be downloaded for free from the CSI Editorial Archives (www.gocsi.com): *"How September 11 impacts your business continuity planning by Carl Jackson"* (http://www.gocsi.com/archive/disaster.html)

Second, consider participating in Infragard (www.infragard.net). InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S.

Would Your Organization Consider Hiring Reformed Hackers as Consultants?



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

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. It has grown to over 3000 members (and 1000 member companies) nationwide.

Dr. Phyliss Schneck of SecureWorks (www.secureworks.net) who serves as both of Infragard's national Vice President and President of Infragard's Atlanta chapter provides some insights.

"The tragic events of September 11th have helped to motivate the private sector to participate more in InfraGard, giving more of their time to security awareness and to participation in their local InfraGard chapters. This energy strengthens overall homeland security. Immediately following 9/11, the InfraGard Executive Board asked the private sector to provide extra support to the InfraGard partnerships and to ensure that meetings and initiatives continued without interruption–even in the absence of some of our FBI partners who were called away to duty on the counter-terrorism task forces. InfraGard is about the protection of an entire nation through information sharing and partnership–starting at the grass roots and connecting to our larger enterprises, policy makers and law enforcement. That has always been the mission of InfraGard, and that mission has remained unchanged before and after September 11. September 11 did not change the mission of InfraGard, yet it certainly reinforced the urgency and necessity for the private sector and government to partner to protect our country.

"Every business is a part of our infrastructure, and there exists a place for every business, independent of size or stature, within the InfraGard partnership. InfraGard membership is a variety of small, medium and large businesses of all types.

"Since we are all connected via the Internet, our electronic and communications infrastructures are only as strong as our weakest links. Any vulnerability, even if in a small business, is a vulnerability that all businesses thus share via transitive connectivity. It is our responsibility and the mission of InfraGard to protect our critical infrastructures from the grass roots / small businesses to the large enterprises.

Third, if the stakes are high enough for your organization, consider e-business insurance.

In April 2002, *Business Week* reported that interest in cyber risk insurance has increased significantly over the past few years and particularly since 9/11.

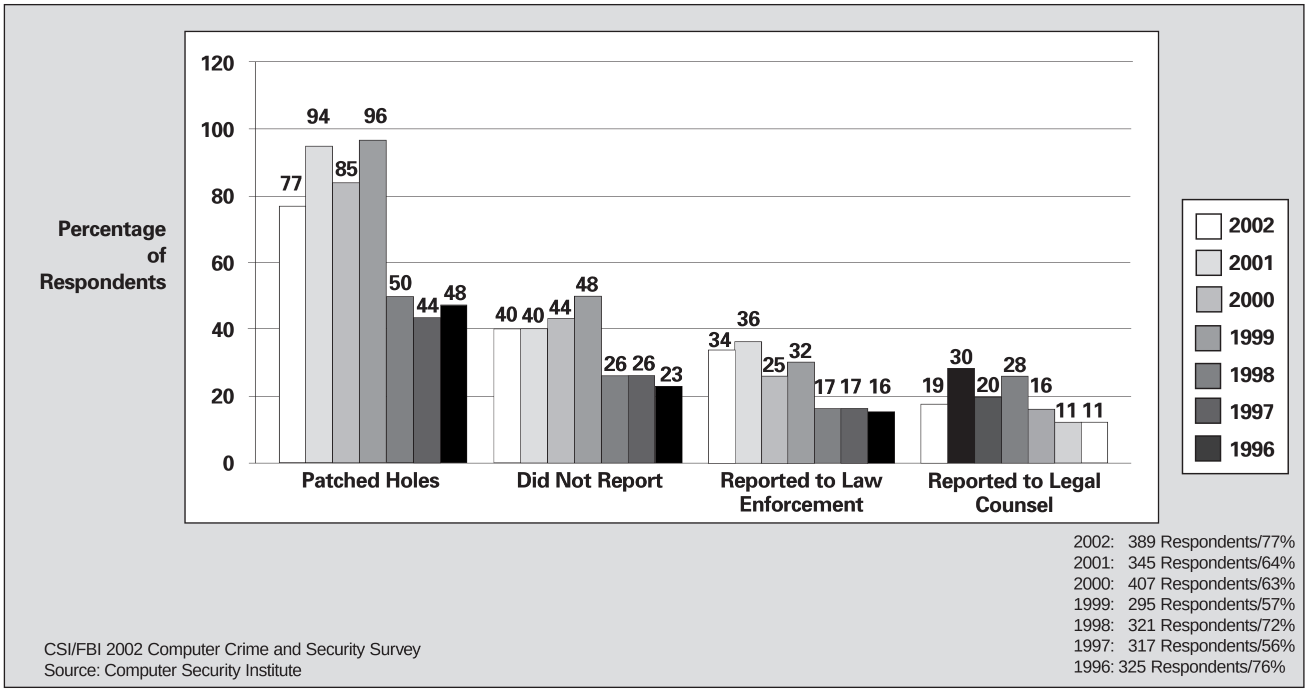
"The past six months have been tough on the insurance industry. Claims resulting from the September 11 terrorist attacks have totaled into the tens of billions of dollars. At the same time, insurers are struggling to recover from a decade of price wars that left reserves depleted. But one tiny part of this sector is going great guns—the e-business insurance market.

"This broad rubric covers policies that address threats new to the Digital Age, including virus attacks, denial-of-service assaults, cracking into company systems, and Web-site defacements. Some companies even write policies that cover cyber-extortion, where an online intruder or an insider steals crucial data such as customer credit-card files and demands a payoff. The rising tide of lawsuits against companies whose employees have used corporate e-mail inappropriately has also caught the attention of e-insurers."

Tracey Vispoli of Chubb and Son (www.chubb.com), agrees with the *Business Week* assessment.

"Several events are prompting more insurers to take positions on covered and uncovered cyber events. Boards of directors and CEOs are becoming better informed about potential information technology exposures that could affect shareholder value. Meanwhile, risk managers are becoming more involved in their organization's IT security and disaster recovery planning processes, heightening their awareness of these new exposures and, ultimately, causing them to reexamine their traditional insurance programs. (see additional commentary below). In many cases, the interest in IT security by CEOs and boards is being driven by the proliferation of laws and regulations aimed at protecting consumer information. Some legislation imposes severe penalties on board members and CEOs who fail to review and approve information technology security plans. Even in the absence of such rules, a board's duty of care requires its members to protect the corporation

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



2002: 389 Respondents/77%
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 2002 Computer Crime and Security Survey
Source: Computer Security Institute

from cyber events that could potentially have a catastrophic impact on the firm's reputation and shareholder value.

"As insurers offer new polices that specifically grant coverage for cyber exposures, they have clarified that coverage gaps exist in traditional insurance policies. Some companies are beginning to learn this the hard way not only as the victims of cyber security-related losses but as the total dollar value of these losses rise significantly. As the CSI survey indicates, while the number of companies reporting cyber security breaches rose 5% in the last five years, the total dollar value of the losses surged from $100 million to $456 million."

"CEOs are now examining cyber insurance as a potential last line of defense. Matching the cost of potential security breaches to the cost of insurance, however, is a daunting task. The potential impact and cost of a cyber event are difficult to imagine because of the unknown, and therefore, difficult to weigh risk-to-reward ratio."

"September 11th has forced companies to plan for the worse and to reexamine their business continuation and disaster recovery plans, both physical and cyber. However, it has also taught us that even the best security or the best disaster recovery plan will not prevent a catastrophic event from becoming financially devastating. Insurance is an important ingredient to assure that a company will have the funds to implement their disaster recovery plan and remain in business. Almost immediately after the collapse of the World Trade Center towers, insurers put claim checks into the hands of scores of devastated companies, which helped to keep them running, set up their disaster recovery plans and meet the payroll needs of their employees and their families."

Fourth, consider establishing a "Chief Security Officer" (CSO) so that cyber security, physical security, personnel security and all other dimensions of security can be rolled up into an enterprise-wide security program. The CSO would have his or her own seat at the table with the CIO, the COO, the CFO, etc.

Phyliss Schneck elaborates.

"A growing trend (that I have seen in mainly large, established businesses) is to empower a CSO to govern both physical and information security. Under that CSO would be the division between the physical and the logical, but the central 'security' reporting structure serves to position information security as a risk management expenditure as opposed to an often forgotten line item in the IT budget. This strategy leaves more room in the IT budget for the sustainability of company systems and core functionality while offloading security to a part of the company that measures, manages and budgets specifically for risk.

"In my opinion, this new CSO position will be a tremendous challenge. That person must take the area of security, which by nature is not a profit center, and drive a strategy for overall success (both financial and practical) in the protection of corporate assets. The CSO is also accountable for anything from an unlocked door to an open network port, so a key challenge for that person is also to assemble an appropriately skilled team to achieve the necessary objectives for securing the workplace, the perimeter, the network, the assets and the company as a whole."

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.

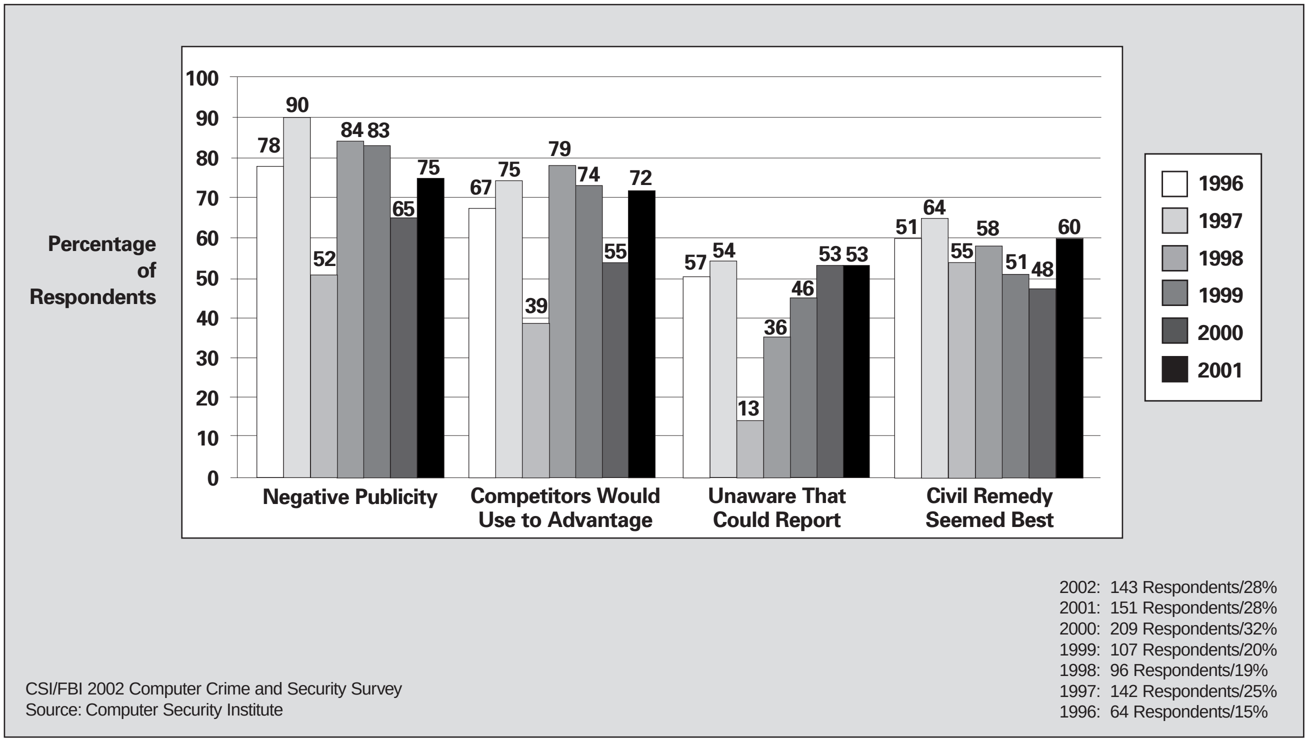
For the first three years, only 17% of those who suffered serious attacks reported them to law enforcement.

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

The Reasons Organizations Did Not Report Intrusions to Law Enforcement



2002: 143 Respondents/28%
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 2002 Computer Crime and Security Survey
Source: Computer Security Institute

enforcement rose again to 36%.

In 2002, the percent of those who reported intrusions to law enforcement held relatively steady at 34%.

The trend is still upward.

In response to last year's survey, Dr. Dorothy Denning of Georgetown University (Washington, D.C.) cited some reasons for the increase of the years..

"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 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 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 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."

Again this year, I urge you to consider Bruce Schneier's balanced view, excerpted from *Cryptogram* in response to the release of the 2001 survey, 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.

"This data is not statistically rigorous, and should be viewed as suspect for several reasons. First, it's based on the database of information security professionals that CSI uses, 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 3,500 information security professionals; 503 responses were received for a 14% response rate.

In 2001, 538 responses were received (14% of 3,900). 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.

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.

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

Network Security Options Making you Dizzy?

attend NETSEC 2002

TECHNICAL DIMENSIONS OF NETWORK SECURITY

Reserve your place today!

SAN FRANCISCO

JUNE 17-19, 2002

HYATT REGENCY EMBARCADERO

For more information go to **www.gocsi.com**,
phone 415.947.6320 or email csi@cmp.com

NETSEC '02

CSI
COMPUTER SECURITY INSTITUTE
www.gocsi.com

FEATURING INTRODUCTORY TRACK, SECURE E-COMMERCE, INTERNET/INTRANET SECURITY, VPNS, REMOTE ACCESS, TELECOMMUNICATIONS, CRYPTOGRAPHY, COMPUTER CRIME, INTRUSION DETECTION & FORENSICS, MANAGEMENT, AWARENESS, INTRO, CISSP EXAM PREP AND MUCH MORE.

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

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

28th Annual Computer Security Conference & Exhibition November 11-13, 2002, Chicago, IL
The world's largest conference devoted to computer and information security

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