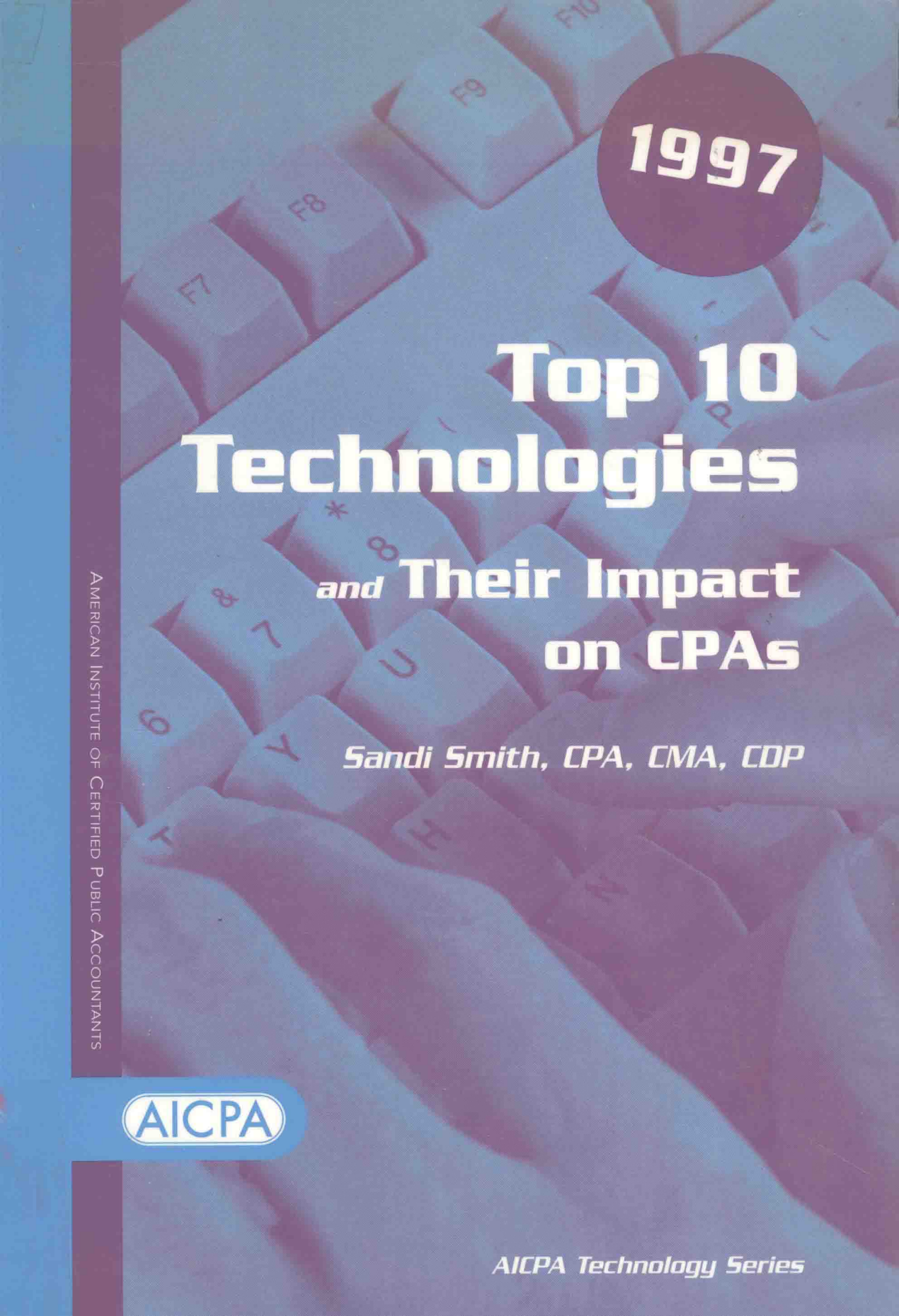


1997

# Top 10 Technologies and Their Impact on CPAs

Sandi Smith, CPA, CMA, CDP

American Institute of Certified Public Accountants

AICPA

AICPA Technology Series


# Top 10 Technologies

## *and* Their Impact on CPAs

*Sandi Smith, CPA, CMA, CDP*

American Institute of Certified Public Accountants

AICPA

*AICPA Technology Series*

# Notice to Readers

*Top 10 Technologies and Their Impact on CPAs* does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the author and publisher are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.



1 2 3 4 5 6 7 8 9 0 PP 9 9 8 7

ISBN 0-87051-184-X

# Foreword

Change is inevitable, and no one should ever fear change. It means opportunity. If you can accept, adapt, and embrace the future—including its quickly evolving technology—you will be able to market yourself as a CPA who can lead his or her clients or employers into the twenty-first century.

The impact of technology on our profession will grow during the next five to ten years at a rate exponentially faster than during the past fifteen years. It is important for you to recognize and familiarize yourself with the technologies your peers identify as being the "Top 10" for 1997. They are the technologies that will have the greatest influence on all CPAs during the coming months. They affect how and when information is created, processed, stored, communicated, acquired, refined, and interpreted. They will change the way you work. They will change the way your clients and employers look to you to add value to information.

This book gives you the needed basics so you can retool yourself to keep up with the rapidly evolving technology and the resulting client needs. There is no questioning the concept that we are becoming more dependent on information systems—*technology*—that rely on little or no human intervention. But there is a limit to what the masterpieces of technology—computers and their related software—can do. You, the CPA, will have to take on the role of consultant, navigator, distiller, analyzer, and interpreter of data. You will have to become the information architect or information professional to bring your clients and employers into the information age. This is the time to grasp the opportunity.

Barry Melancon, President
American Institute of CPAs

# Table of Contents

**SECURITY**

# technology 1

There is no shortage of sensational headlines in articles reporting security breaches of computer systems:

"*Air Force Web Site Shut as Hackers Gain Access, Change Files:* Hackers . . . broke into the site. . . shut down 80 other sites. . . put pornography pictures on our site."[1]

"*Cops Versus Robbers in Cyberspace:* . . . $15 billion loss to the U.S. software industry due to illegal copying . . ."[2]

"*Hack Attack: Cyberthieves Siphon Millions from U.S. Firms:* . . . losses due to hacking, bribery and . . . industrial espionage . . ."[3]

"*Electronic Vandals Tamper with Web Pages:* Graffiti artists . . . Web pages defaced . . . blatant mischief or malice . . ."[4]

It's no wonder that CPAs voted security as the top technology issue affecting their profession. The objective of keeping the wrong people *out* and the right people *in* your organization's computer systems is increasingly challenging.

Several factors over the last few years have contributed to skyrocketing losses from breached security. The trend of companies networking an increasing number of computers has given individuals access to more information than ever before. As companies use technology and change their organizations accordingly, a large number of individuals are being displaced through layoffs. Some of the laid-off workers have grudges large enough to incite crimes against their old organizations. And for the employees lucky enough to remain after the layoffs, loyalty is at an all time low.

Giving employees access to the Internet increases the complexity of networks and increases the chances of unwanted intruders. Some companies do not even know when uninvited hackers infiltrate their networks. Many breaches go undetected because network administrators do not monitor the traffic or do not have the right tools. Even if a company was aware of a security breach, it might not report the activity. Companies are concerned with adverse publicity concerning these intrusions.

Information systems managers have their hands full. Two surveys show that about half of the survey participants, mostly large firms, experienced an information security breach during 1996.[5,6] A recent survey by Ernst & Young shows that a whopping 78 percent of the companies surveyed

incurred losses due to breached information security and disaster recovery. The largest cause of the losses was from those pesky, unwanted viruses.[7]

The first part of this chapter describes today's threats to computer systems. The next part of the chapter is about prevention. All companies should have a comprehensive information security policy that addresses (1) mundane yet crucial areas such as backups and disaster recovery and (2) the use of high-profile penetration-prevention tools such as firewalls and encryption.

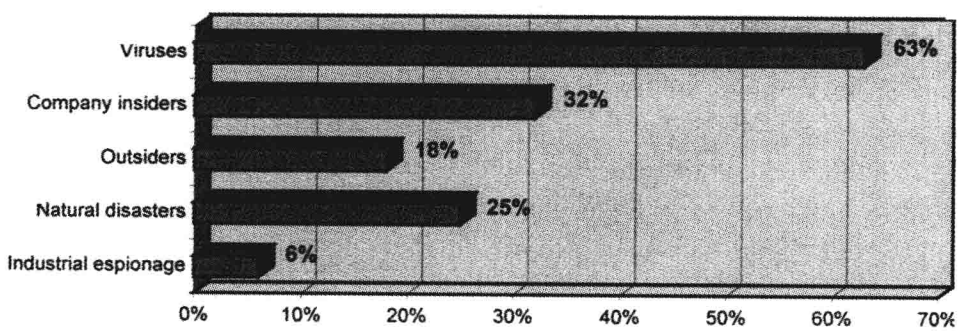
The last section of this chapter presents two more topics related to security: software piracy and consumer privacy, the latter of which includes a discussion of "cookies" (bits of files containing information about website visits).

## THREATS TO INFORMATION SECURITY

The most common threats to corporate information systems are—

1. Viruses.
2. Computer crime caused by
   a. Employees.
   b. Hackers.
   c. Competitors.
3. Natural and man-made disasters.

**FIGURE 1.1: LOSSES DUE TO INFORMATION SECURITY AND DISASTER RECOVERY**



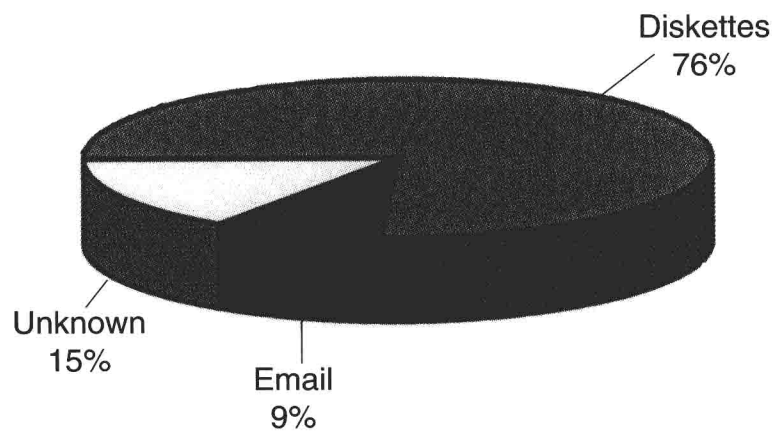
## Viruses

No one wants to get a virus on his or her computer. Viruses are programs that we do not invite into our computer systems, but they crash the party anyway. Often, when they run, they do nothing. But sometimes they wreak severe damage to files and data on our computers by deleting work or rendering it unusable. Who writes viruses? I'm sure there are dozens of theories on the answer to that question, but the bottom line is that they are criminals. Writing viruses that destroy data is a crime.

1996 was a busy year for viruses. New, damaging viruses, such as the *Word.concept* (Word macro) strains and the *Hare* (as in Hare Krishna) virus, made headlines and spread faster than viruses had ever spread before, with networks and the Internet speeding the contagion.[8] 1996 was also a busy year for antivirus software. The guys and gals in the antivirus software labs kept up with the maddening pace of new viruses. They used sophisticated "bloodhounds", such as neural networks, that could sniff out and snuff out brand new viruses before they spread.[9] 1996 was a busy year for companies that suffered losses from computer viruses: the total was expected to reach between $2 billion and $3 billion.[10]

How do companies' systems get infected with viruses? The most common source of a virus infection is diskettes. Viruses hide in files on diskettes that we carry from machine to machine. Viruses can also hide in email. Infected email is a relatively new source of worry for companies because of the creation of the Word.concept virus in 1995.[11]

**FIGURE 1.2: SOURCES OF VIRUSES**



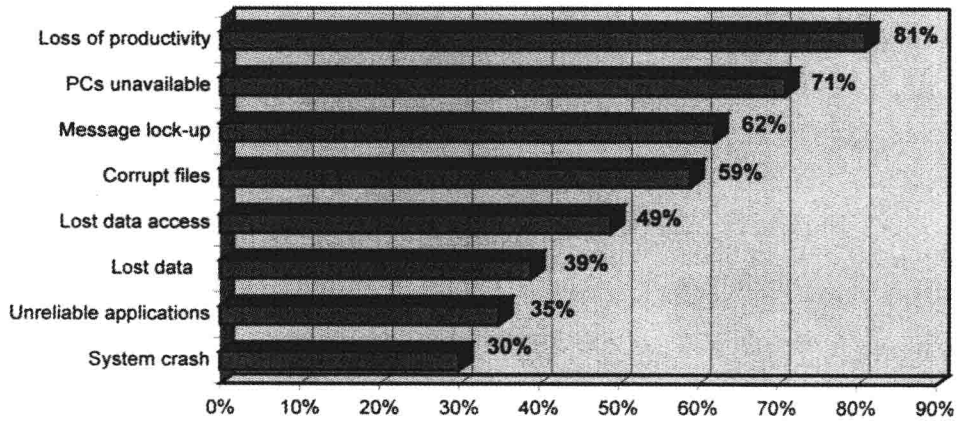
Companies that have suffered from virus attacks have reported losses in productivity, losses in the use of PCs, and losses of data.[12]

Only a small percentage of viruses actually damages data. The Word.concept virus is by far the most common virus that appears now, occurring in 49 percent of all virus incidents.[13] Of the dozen or so mutations of this virus, only a few of them corrupt or destroy data. One strain converts Microsoft Word document files into document-template files and renders them basically useless. Others display a message or freeze a system. PCs at a weekly newspaper "caught" the *Wazzu Word macro* strain last year, shutting down production for two days. The virus did not destroy data, but did cause a great deal of disruption.[14] Antivirus software is effective against the Word.concept virus.

The Hare virus is particularly evil. It strikes on August 22 and September 22, displays the message "HDEuthanasia", and proceeds to overwrite hard disk files. Another version of macro viruses called *ExcelMacro.Laroux* infects Microsoft Excel spreadsheets and can travel via email.[15]

Although the vast majority of viruses do not destroy data, they can be just as disruptive to productivity. Another "form" of virus that drains productivity is the rumored virus, or hoax virus. These viruses do not exist but somehow a rumor has circulated about their upcoming appearance. Reports of hoax viruses are becoming increasingly common. Information systems personnel must investigate each report, zapping precious resources. Some of the viruses that do not exist have names and have been circulating for years: the *Good Times* virus, the *Deeyenda* virus, and the *Irina* virus

**FIGURE 1.3: LOSSES DUE TO VIRUSES (MULTIPLE RESPONSES)**



(which was a marketing stunt). Reports that a *Ghost.exe* virus will destroy a hard disk are false: it is a screen saver that is activated on a Friday the thirteenth.[16]

Until the creation of the macro viruses, the most common type of destructive virus was a boot sector virus, named for the part of the computer system it infects. The boot sector contains the commands that the computer sees when it is turned on and is especially vulnerable to an attack.[17] Companies' prevention programs must take into account this type of virus, which is detected by periodically scanning the boot sector of the computer. A scan of all files on a hard disk will reveal other types of viruses, and a scan of email files will detect even other types of viruses.

## Computer Crime

The frequency of losses due to theft of proprietary information has surged in the last three or four years. A survey from the American Society for Industrial Security (ASIS) describes what types of information are commonly targeted:

- Strategic plans
- Research and development information
- Manufacturing processes
- Marketing plans
- Intellectual property
- Financial data
- Merger/acquisition data
- Customer lists
- Personnel plans[18]

The most common breach of information occurs not by computer systems break-ins, but over the telephone. An outsider will call an employee and get the information sought by acting like someone else. Figure 1.4 presents how information is stolen, based on the ASIS survey.[19]

In this section, we'll discuss the classes of individuals most likely to perform computer crimes. The list includes—

- Employees, ex-employees, and other trusted parties
- U.S. and foreign competitors
- Hackers[20]

**FIGURE 1.4: HOW INFORMATION IS STOLEN IN COMPANIES**

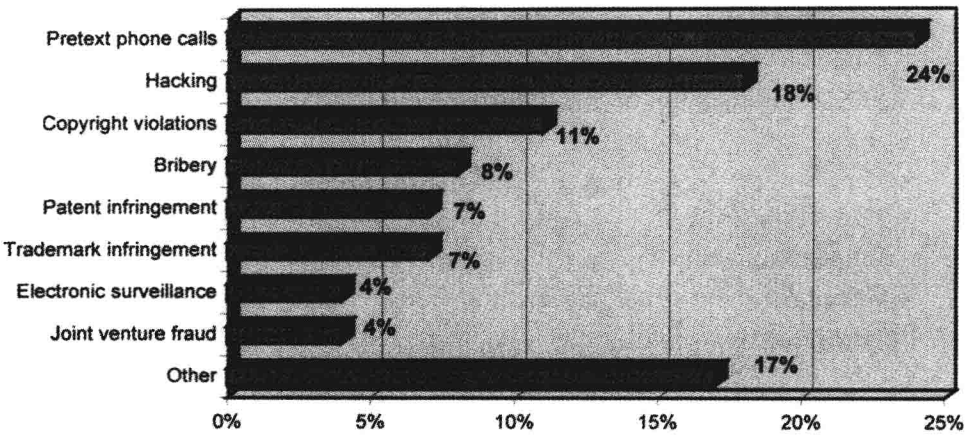
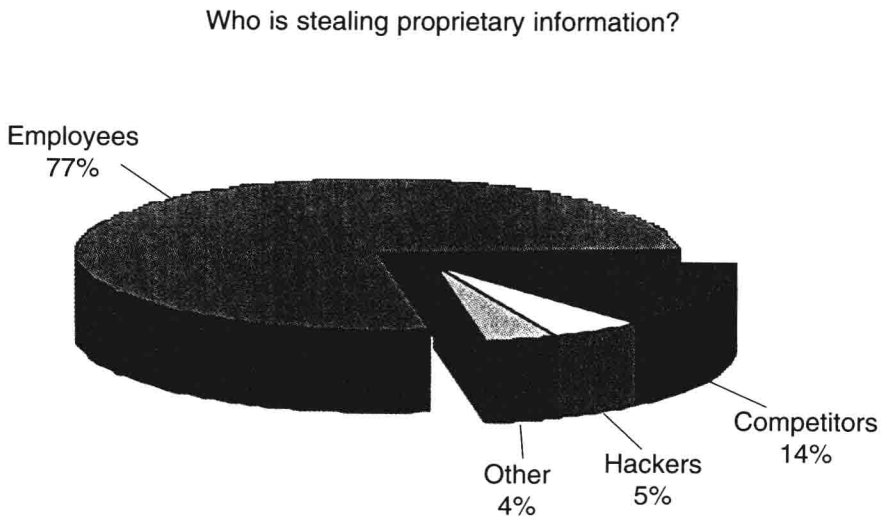



**FIGURE 1.5: EMPLOYEES TAKE THE LARGEST PIECE OF THE PIE IN STOLEN CORPORATE INFORMATION**




## Employees

Believe it or not, one of the most damaging enemies to corporate information lurks inside corporate walls. Seventy-seven percent of information is taken by employees and other trusted parties.[21] Frank Clark, a criminal investigator who once cracked a murder case from evidence

stored on a hard disk, puts that percentage a little higher. He says that 80 percent to 85 percent of computer crime losses are inside jobs.[22]

William Gaede, who worked for Intel, tried to download files that contained the blueprint for the Intel Pentium chip. He couldn't because of security limitations. But he could display the blueprints on his computer screen. He then proceeded to videotape them. He left the United States with the videos and was arrested for transportation of stolen property and mail fraud.[23]

In some people's minds, computer crimes do not seem as serious as other physical crimes, like breaking into a building. In the comfort of home or office, a person can "peek" into a confidential file or email. The same person would not dare steal a car or break into a house, but might be tempted to read a private email or sift through unauthorized files.[24]

What types of employee engage in these acts? It's not always easy to identify them, but Frank Clark lists some common traits. These employees typically—

- Are low wage earners with little or no investment in the business.
- Spend a lot of time on the computer.
- Sometimes exceed their authority.
- Might have a grudge from losing a promotion or from some other work-related disappointment.[25]

With the waves of downsizing occurring in the last decade, there are armies of former and current employees who have lost their drive to be loyal and who might have just enough of a grudge to act when the situation arises. Ernst & Young warns against keeping terminated employees on-site as a result of relocation package benefits that include the use of an office for a period of time. One disgruntled employee is all it takes to impart considerable damage to corporate information.[26]

## Competitors

It is easy to obtain information on your competitors without breaking any laws. A company's Web site is a good first stop. But for a few companies, that's not enough. The number of incidents of companies stealing information from their competitors is higher for cutthroat industries, such as high technology. Industries with large contracts that involve a bidding

process in which millions or billions of dollars are at stake are ripe for this type of crime.

One notorious case between competitors Borland and Symantec lasted four years before it was resolved in late 1996. Eugene Wang, a Borland employee, allegedly supplied Symantec with Borland's product marketing plans. Then he went to work for Symantec. Borland filed suit against Symantec.[27] The case never reached trial because of a questionable $13,000 contribution from Borland to the district attorney's office and other legal issues. It was dismissed in November 1996, primarily because of its loss of relevance due both to the age of the dispute and to changes in California law.[28]

Another case involved two competitors, Cadence and Avant!, that sold systems that designed integrated circuits. It started with a Cadence engineer who acted suspiciously during his last days of work. When the police raided the engineer's apartment, they supposedly found source code owned by Cadence. Later, a Cadence employee who helped a customer that ran both Avant! and Cadence products noticed a programming bug in the Avant! software that was identical to one in the Cadence software. The police confiscated Avant!'s files and programs, and Cadence filed suit against Avant! for copyright infringement. Avant! filed against Cadence for damaging its business reputation.[29]

It is not unusual for employees to be "double agents" at some companies where multibillion dollar bids are at stake. An employee of Company A, who is really working for Company B, can provide Company B with valuable details about how Company A is bidding. A coincidence when two bids come in only $1,000 apart? You be the judge.

### Hackers

A small percentage of our population is made up of criminals. They rob grocery stores and gas stations; they sell drugs; they may commit worse crimes. Some criminals came with us into cyberspace: these people are called hackers. They are the criminals of the computer world. They rob companies of information, compromise systems, and perform fraudulent acts. The most common things hackers do, according to a survey by WarRoom Research LLC, are listed below:[30]

- Probe/scan systems— 14.6%
- Compromise email or other documents— 12.6%
- Introduce virus— 10.6%
- Compromise trade secrets— 9.8%
- Download data— 8.1%
- Change data— 6.8%
- Install password sniffer— 6.6%
- Deny use of service— 6.3%

Hackers can penetrate security in many ways. They can intercept Internet traffic, such as files or email. They can attempt to break into a private network. They can even reach into your own computer files from a Web site that you are visiting by using an applet that is received by your browser software. In the last case, both Microsoft Internet Explorer and Netscape Navigator allow Java, ActiveX, and other applets to run commands on your computer. Each time new security holes in the browsers are discovered, usually by the computer security teams at Princeton University, Microsoft and Netscape issue software fixes very quickly. The only way to totally prevent this possible breach is to turn off Java and ActiveX capabilities in the browsers.[31]

Hackers are generally young, in their teens or twenties. For most, hacking is a way to play pranks on people. Some see it as revenge. Others see it as a brag or a challenge: each intrusion is a "notch on the bedpost," according to a seventeen-year-old hacker from Newark, California.[32]

Hackers like to make their mark on Web sites. The site of the American Psychoanalytic Association was broken into by a hacker trying to impress his girlfriend. It took a week for the Web site of the Nation of Islam to be cleaned up after a recent attack by unidentified hackers.[33]

The government is a constant source of amusement for hackers. Over the 1996 Christmas holidays (a favorite time for hackers) the Air Force Web site was penetrated. Hackers replaced military service fact sheets and commanders' biographies with a sexually explicit video and a claim that the government lies to citizens. During summer 1996, an image of Hitler and a swastika appeared on the Department of Justice's Web site, courtesy of hackers. In autumn 1996, the Central Intelligence Agency's Web site was renamed "The Central Stupidity Agency" and garnished with adult photos.[34]

Most actions by hackers are nuisances that do not pose any real threat. But hackers have skills that should not be taken lightly. A few companies are hiring them to find holes in their security systems. Hired on as a temp, one hacker accessed the company's $1 billion project files in his first few hours on the job. He printed fake business cards, hooked up a portable Unix to its network, and forged the president's digital signature on documents. He was successful at extracting legal, licensing, and top-secret data, and built himself a trapdoor so he could return in the future.[35]

Frank Clark urges companies not to hire hackers. He says the basic nature of people is simply not going to change, and a company does not have enough skill to police hackers, even in its own environment.[36]

The attitude of the hacker community is getting scary, even to former hackers. One twenty-year-old reasons that if a network administrator who is paid $60,000 a year or more cannot keep the network secure, then the company deserves the intrusion. Other hackers just sit around formatting hard disks (this erases everything on the disk) to make people angry.[37]

## Natural and Man-Made Disasters

Mother Nature can deal her hand occasionally. Whether it's a fire that wipes out one company or a hurricane that wipes out a city, corporations must protect themselves from the possibility of a disaster. Periodically, a company data center must be rebuilt because of a man-made disaster such as the Oklahoma City bombing.

In all of these cases, off-site storage and backup data centers play a major role in getting online again quickly. In one case in Oklahoma City, the off-site storage area containing backups of the company's data was across the street from the company's building. Both were damaged in the bombing. In this case, the off-site backup was not far enough away to make a difference.

In early 1997, floods in the western United States proved a challenge for some systems staff. Companies with a solid plan stayed dry. The systems personnel of The Hampton Inn in Reno, NV, placed its equipment on racks while four feet of water swept through the downtown area. The network was brought down in a normal shutdown procedure, and critical systems were moved to the designated backup site. Reservations continued to be taken and honored without a hitch.[38]