

June 15, 1998

Cyber Sabotage

Elements of Workplace Violence in Computer Crimes

Workplace violence traditionally conjures images of the disgruntled employee or former employee who arrives at work with a loaded gun and a deadly vengeance. The spectrum of workplace violence, however, starts much less dramatically, beginning with employees who disrupt the workplace through small-scale sabotage and vandalism to those who intentionally destroy company assets and assault their co-workers. While it is impossible to accurately predict which employee will resort to physical violence, experts believe the most likely candidates for workplace violence are persons who have low self-esteem, do not feel valued, fear for their jobs or promotions, are frustrated, or have a negative attitude toward management.

In recent years, more and more employees, motivated by such feelings of bitterness and frustration, are exercising their violent tendencies by lashing out at the company through the computer. Employees are discovering that tampering with company computers or using the computer to steal are more convenient and less risky ways to vent frustrations on their employer.

Most companies have millions of dollars invested in their data, computer hardware and software, yet the 1998 Computer Security Institute study shows most firms do not have controls or policies in place to protect one of their greatest assets—information technology—against one of its greatest threats—employees.

The Insider's Crime

Over 90 percent of economic computer crimes are perpetrated by a company's own employees, said the United Nations Manual on the Prevention and Control of Computer Related Crime. While studies do not put the percentage as high as the United Nations manual, the impact of worker-inflicted damage to computer information is great enough for the UN to characterize computer abuse as "the insider's crime."

Anger at his supervisor and fear that he would lose his job prompted the designer of a new razor to send out plans electronically to company competitors. The loss of this strategic and proprietary information to his employer was \$1.5 million.

The financial impact of insider computer crime is staggering. Experts believe using a computer to

commit fraud costs business an estimated \$3 to \$5 billion a year alone—and only five to ten percent of estimated losses are reported. When a publication surveyed 1,225 businesses in 1997, those that responded reported a median loss of \$10,000 for each incident of abuse by an employee. Just under half the respondents said they suffered at least one incident of information misuse within the year, including unauthorized access by an authorized user, leak of confidential information, or destruction of data.

Employee sabotage of information and information systems can include theft, fraud, destruction of data, corruption of data or software, or any act which deprives a company of its rightful access to information. The sabotage can also include unauthorized use of information and information systems for personal gain or entertainment, with motives ranging from revenge to accepting a technical challenge.

The fastest-growing computer-related crime is theft—and one of the most commonly stolen items is information, according to experts. One East Coast firm lost \$1 million worth of proprietary information to an employee who found a way to connect his modem at home to his company computer network. For three months he diverted copies of e-mail, interoffice communications, confidential correspondence about company projects, personnel and sensitive customer information.

While money still makes up a large amount of stolen goods, a 1996 study of computer crime conducted by two professors at Michigan State and Wichita State Universities showed the most common items stolen from companies were new product plans, new product descriptions, research, marketing plans, prospective customer lists and similar information. The study found insider thieves preferred stealing from computers "because it provides more extensive access to more usable information, is easier and more reliable than other methods, and presents less risk of

(continued on next page)

Cyber Sabotage

Elements of Workplace Violence in Computer Crimes

(continued from preceding page)
detection and capture.”

Embezzlement and fraud are also easier by computer. “Computers offer embezzlers with some computing and accounting skills an easy way to steal and make their crime harder to detect and prosecute,” said one expert in embezzlement. At one large company an employee in accounts receivable entered incorrect figures in his computer to allow a customer to avoid timely payments and earn some \$2.1 million in interest. The customer paid the employee kickbacks. But computerized embezzlement is not just the province of large companies, A 22-year-old worker at a fast food restaurant reprogrammed the computerized cash register in his drive-through window to ring up each \$2.99 item as a one-cent item. He embezzled \$3,600 before he was arrested.

Motives

Personal gain is not always the object in attacks on information systems. Other motives range from a desire for revenge to fear of job loss:

- A worker in Canada, denied a weekend off, hit a few keys on a computer and six months worth of data disappeared.
- A disgruntled hospital employee accessed computerized medical records and published a list of HIV positive patients.
- Another employee who didn’t get paid for a meeting he attended put a virus in the computer.
- A man who feared he would soon be out of a job programmed the company computer to delete the customer database when his name was taken from personnel records.

Malicious acts by insiders account for many incidents of computer sabotage. An accounting firm surveyed North American companies in 1996 and discovered one-third lost valuable information over the previous two years to malicious acts of insiders. Such acts usually happen when the empowered become the embittered—when workers, out of

sheer boredom or inadequate training, turn their computers into tools of mayhem. Commonly, employees plant viruses as games, a prank or a challenge, but management must take these computer intrusions seriously, said one accountant who studied the problem. The employee who connected his company network to his home computer and cost his firm \$1 million began his illegal activities merely as an intellectual challenge.

Employee abuse of information assets stems from the same factors as workplace violence to persons, said a former FBI official who worked with the agency’s computer systems and is an expert in fighting computer crimes. “The violence is inflicted as an attack on the assets of the organization,” he said. “Typically it is an unhappy employee who acts out aggression or simply acts less physically violent, but at the same time is violent.” He added that erasing a company’s valuable records with a keystroke has the same impact as demolishing the firm’s computer room with a baseball bat.

Unlike swinging a bat, most cyber-criminal acts appear to be part of a worker’s normal routine. Often weeks or months pass before the company realizes there is a problem. At one large bank, an unknown employee programmed the computer to transfer 12 to 25 cents periodically from hundreds of accounts into a bogus account. In a year the figure amounted to tens of thousands of dollars which was then withdrawn—and never seen again.

Whatever the motive, the economic impact of employee attacks on company information and information systems cannot be underestimated. Companies today are so dependent on computers that the loss of critical cyber-support or part of that support could ruin a business. Small to mid-sized companies overwhelmingly do not recover from major losses of data or computer loss, according to a study by two certified public accountants who deal with disaster recovery. The average company that does not have its computer system operating for six days experiences a 25 percent

loss of revenue, experts report. Within two weeks of losing computer support 75 percent of organizations reach critical—or total—loss of functioning.

Curbing Computer Sabotage

Corporate executives agree that employees tampering with the computer system or its data present a significant problem, but they seem uncertain how to contain it. Half the corporate spokespersons surveyed for an international report on business computer security said the greatest threat to their company's cybersecurity comes from former employees and unauthorized users within their companies—and 74 percent believe their information security risk is increasing.

Effectively curbing computer sabotage must begin with education and effective management, experts agree. First, security and human resources managers should know the opportunities and motives that contribute to employee sabotage and workplace violence. Second, employers must adopt strict computer use policies and make employees aware of these policies.

Studies show some corporate cultures seem to contribute to workplace violence and employee abuse of computer systems. Management experts and former law enforcement officials say high stress levels within a company, problems between labor and management, weak internal controls, or ineffective supervision of employees seem to foster problems.

Security managers who recognize that elements in their corporate culture might contribute to computer sabotage should also look for danger signs in employees. Security managers should be alert to employees who work at the company and have:

- Demonstrated dissatisfaction with salary, promotion opportunities or working conditions;
- Conflict with managers;
- Financial problems which may be linked to alcohol or drug abuse.

Procedures should be in place that allow employ-

ees to alert security management to those who:

- Stay late or arrive early to work;
- Never take a vacation. Fraud and embezzlement require constant attention to cover;
- Have independent access to information and information systems;
- Feel pressured to pay for costly medical treatment for a spouse, child or loved one.

Preventive Measures

Once the degree of danger is assessed, security managers should be given the resources to develop plans to protect the company's information system against an internal attack and recover lost data if an attack happens. Every company should have a policy that clearly states how the computer will be used. The policy should be widely publicized.

At minimum, a computer use policy should: discuss in detail how the Internet can be used and the proper reasons for Internet use; involve passwords that an employee memorizes and does not share with anyone; limit employee access to computer files; make the company computer network a group project and never leave one employee in charge of major portions of the network list; outline clearance requirements for employees who work in sensitive areas; and provide well-defined lines of employee supervision and authority.

Information security specialists recommend these additional safeguards: develop an emergency plan to handle varying levels of computer loss; develop methods of tracking patterns of information use; establish a compartmentalized computer network that makes it very difficult for employees in one department to view or work on files from another department; back up files and important applications by sending copies to a separate physical location; and keep computers behind locked

(continued on next page)

Cyber Sabotage

Elements of Workplace Violence in Computer Crimes

(continued from preceding page)

doors when not in use.

Once the policies are in place, security managers and company officers should adopt a “zero tolerance” stance against violations. This does not mean every infraction should mean dismissal. However, every offense should be noticed officially and brought to an employee’s attention. The Computer Security Institute study showed companies do not want to risk public embarrassment by cooperating with legal authorities, nor do they want competitors or customers to know their computer systems could be compromised. But “zero tolerance” should involve cooperating with authorities to apprehend and prosecute employee computer criminals.

If prevention is the most practical answer to computer sabotage, the most important element in the security of information systems is careful hiring, experts agree. Organizations should perform careful background checks that include references and criminal records. Where permitted, employers should require drug testing for all employees who work with sensitive information.

On the other end of the employment spectrum, companies need termination policies that do not permit a former employee to access the computer system. FBI officials and employee-relations managers advise companies to keep employee lists up to date so security officers can check for terminations and prevent these people from entering the premises. In addition, a termination policy should: give the terminated employee notice, have a security officer and human resources representative watch the employee clean out his or her desk, then escort that individual to the door. In some locations, the company may have to provide an employee with two weeks’ severance pay, but workplace violence experts say this is better than letting that person stay and potentially cause millions of dollars in damage.

Employee sabotage of computers and computerized data is now a fact of economic life that

companies must learn to manage.

Prevention is the least costly solution to computer sabotage today. Most companies have millions of dollars invested in their computer hardware and software, yet they do not have security in place to protect one of their greatest assets: information technology.

Security managers should form teams with information systems specialists and human resources managers to study the risk exposure of their companies and make top management aware of the internal situation. Security managers will play an increasingly important role in developing policies addressing employee abuse of information and computer systems.

A firm, clear policy on the use of computer technology will help clarify issues for employees. Make certain the policy is well publicized and adopt a “zero tolerance” stance for violators. Employers must be willing to prosecute employee criminals and weigh any bad publicity against the deterrent value. Congress provided an invaluable tool for punishing anyone who sells trade secrets in the Economic Espionage Act of 1996, which explicitly made the theft of trade secrets a federal felony. Prior to this law, the FBI and other law enforcement officials had to rely on general statutes such as interstate theft of stolen property and “fraud by wire” to prosecute thefts of high-tech secrets. Successful prosecution, however, requires that employers break the prevailing silence and cooperate with law enforcement.

In light of this growing threat, companies can no longer ignore the problem of internal computer sabotage in hopes that it will go away. Organizations must recognize the danger and educate their workforce—from the most senior manager to the newest employee. Perhaps even more important, however, is the need to work with law enforcement to prosecute violators. By removing this veil of silence, employers remove one of computer criminals’ greatest allies.



The Lipman Report Editors