



saleswoman at Chicago's O'Hare airport was making a few telephone calls before catching her connecting flight home on a Friday afternoon.

As she punched in her access code, she looked over her shoulder at what appeared to be a tourist videotaping a farewell to friends. Upon arriving at the office the following Monday, she found every telephone line busy.

A management investigation and tap into the lines discovered that most of the conversations were not in English. It took hours to shut down the system. The final tally: \$530,000 in toll calls over the weekend, most of them to Latin American and third world countries.

Our salesperson was a victim of "shoulder surfing", criminals looking for credit card and telephone system access numbers. Videotaping enables these thieves to play the tape over and over until the correct code is deciphered. You, the risk manager for the victimized firm, are asked by your chief financial officer to present this to your insurance carrier. To your horror, the property and the crime carrier both tell you this is not covered. An unlikely set of circumstances? Most experts, including the Secret Service, estimate that losses from toll fraud exceeded \$1 billion in 1993.

IS IT COVERED?

Standard crime policies cover employee dishonesty, forgery, money, securities and computer fraud (actual transfer of money or property using a computer). Property policies cover theft of *tangible* property only. *Black's Law Dictionary* defines tangible property as: "That which may be felt or touched and is

necessarily corporeal ...". Even if you could convince your carrier that unauthorized toll charges are tangible property, it would most likely tell you that it is an off premises theft, subject to a sublimit.

Why is PBX fraud a growing crime? What is PBX fraud? PBX stands for private branch exchange, which is customer owned or leased telephone equipment. Criminals have finally caught up with technology, and the black market is hot for stolen credit card numbers and access codes. What is more, sentences for convicted toll fraud criminals are relatively lenient.

Organized groups of these high tech criminals are now in Europe. Not only do they practice their trade in their own countries, they routinely break into American systems and steal the codes.

CALL-SELL OPERATIONS

I testified at a Federal Communications Commission (FCC) hearing on telephone fraud. Witnesses described the popularity of stolen codes among organized crime and drug dealers. Codes are also widely used in call-sell operations springing up in most large cities. Criminals operate call-sells by renting an average size store and installing, for example, 30 telephones. A user pays an up-front fee, usually \$15-\$20. The 'customer' is given a stolen credit card or PBX number allowing him to call anywhere in the world. The call-sell manager usually allows the 'customer' to use the phone for 15 or 20 minutes.

TELEPHONE FRAUD: REACH OUT AND ROB SOMEONE

by Frank Scheckton Jr.

People, who are in this country illegally, or for whatever reason cannot get a phone, rely on operations like this. In some cities, one can actually see people in line at telephone booths with others nearby timing them with stop watches!

PBX FRAUD

Travelers Crime Division first heard about PBX fraud in 1983 when one of its customers, a Fortune 100 corporation, submitted a claim for \$382,000 in unauthorized telephone calls. Almost all of these calls were to the Dominican Republic and Columbia — still very popular destinations for many PBX fraud calls. We paid this claim under the customers' fidelity (employee dishonesty) coverage. Our customer proved that two of its employees were selling the direct inward system access (DISA) code of the PBX system on the streets of New York City.

DISA enables you to call your company, punch in an access code and make outgoing telephone calls at a rate that is usually cheaper than a calling card. Our customer told us they were not even aware their system had a DISA feature.

It is not uncommon, based on my experience over the past several years, for companies to be unaware of the full capabilities of the equipment they purchase. More than half of the victims we spoke to told us that they were never warned by the vendor that losses of this type could happen.

Since Travelers introduced its telephone fraud policy in August 1992, hundreds of victims have contacted us to tell us about their experiences. Some things have not changed since 1983. The Caribbean Islands and South America still seem to get the lion's share of illegal calls. The thieves are organized criminals, drug dealers and call-sell operators. What is starting to change is how we view high technology crimes.

John J. Haugh, author of the two volume, *Toll Fraud and Telabuse*, refuses to refer to perpetrators of telephone fraud as "hackers." These are not college kids trying to break into systems for the thrill of it. Some of these individuals are on \$10,000 a week retainers.

Others are paid \$100 to \$300 for every cracked code they can come up with. Since a constant supply of new codes are needed, these criminals have a steady source of revenue.

There is great debate about the average loss amount. Mr. Haugh indicated \$168,000 in his book. Based on Travelers' discussions with victims and testimony at the FCC hearing, \$160,000 seems about right. Mr. Haugh says that 35,000 systems could be compromised in 1993. According to the Secret Service, it is not a matter of if, it is a matter of when. That is frightening when you consider that there are more than 180,000 systems in the United States alone.

Horror stories abound. Some of the more notorious cases: Mitsubishi — \$430,000; United Nations — \$900,000; AVNET — \$500,000. Ironically, the US Drug Enforcement Agency reportedly suffered a loss more than \$1 million. Although we cannot release information contained in the applications of our customers, it illustrates that high technology criminals are getting more sophisticated.

Telephone thieves are not just concentrating on the DISA. They can get into your system through voice mail, the auto attendant or the remote maintenance port of your computer. The auto attendant is the computerized voice that answers the phone and prompts callers on what numbers to press.

Remote maintenance and testing system ports (RMATs), allow users to change software, direct the hardware being used and perform diagnostics when something appears wrong. In other words, a system can signal a repair technician or owner saying: "Call me, I'm sick." The technician can call the system back through the maintenance port and ask what is wrong. The only thing not known is how to send chicken soup!

We learned of a situation where, on a Friday night, the criminals came into an insured's system through the maintenance port, locking out all of the other access codes and creating a new one for their use.

To cover their tracks, they disabled the station message detail reporting (SMDR), a highly recommended device that stores information such as what number was dialed and length of the call. Since this customer had been victimized before it had attempted to control further losses by allowing only a small portion of outgoing telephone extensions to make long distance calls

That restriction was quickly done away with once the criminal got into the program. Over the weekend, more than 6,000 calls were made. When the victim opened for business on Monday morning, all of its lines were busy and the company denied access to its own system.

It frantically contacted the vendor since it is common for programmers to leave "trapdoors" in their program to allow them access. These sophisticated computer criminals also had closed the trapdoors, lending credibility to the theory that some perpetrators out there are former employees of vendors and telephone carriers. This victim had only one choice: disconnect the equipment and shut down the system. The resulting loss of business was estimated to be almost as much as the cost of the calls.

WHO IS RESPONSIBLE?

Some victims of telephone fraud have refused to pay their bills. They argue that the calls were not made or authorized by them. Others have compared the PBX to a stolen car used in a bank robbery. Is the owner of the car responsible for the stolen money? Some victims have sued their vendors claiming they should have been warned about the dangers of remote access fraud. One particularly amusing response was a vendor comparing their equipment to that of a sports car. Is the auto dealer obligated to warn the buyer that the car is capable of killing him?

Sentiments ran high at the crowded FCC hearing in October 1992. Good arguments were certainly made for both sides. As a representative of Travelers, I was asked to speak on telephone fraud insurance, as some people look to insurance as a possible solution.

Based on submissions to Travelers Crime Division received so far, insurance is not a panacea.

Some risks, for a variety of reasons, will never be insurable. We have had customers tell us that they will not force their employees to use passwords with more than three digits because their people cannot remember them! Other companies say they will not limit unsuccessful log on attempts because their executives have fat fingers and often hit the wrong keys. When we advised one firm to limit access on weekends, it decided against it. All of these are business decisions. However, we conclude that all risks may not be insurable. Insurance may help, but it is not the answer.

THE REGULAR ENVIRONMENT

Industry insiders hoped that a trial court decision in the Mitsubishi lawsuit would resolve the question of who is responsible. The case was recently settled without a decision, rumored to be based on an agreed upon percentage of the bill. One recent decision that has received a lot of attention is *AT&T v Pacific Mutual life Insurance Company* heard in California Federal District Court.

Criminals on the east coast hacked into Pacific Mutual's PBX and made long distance calls, primarily to South America. District Judge Irving Hill's decision was that the ATTs Tariff One was not unambiguous and that the calls originated from Pacific Mutual's PBX. Pacific Mutual was liable for approximately \$170,000, including interest.

In September 1992, Congressman Edward Markey (D-Mass) introduced a bill that would have required the FCC to establish rules to protect consumers from telephone toll fraud. Provisions of the bill would have required manufacturers and vendors to warn customers about the possibility of toll fraud and advise them on safeguards. The bill, which was not passed by the end of the 102nd Congress, would have limited the end user's liability to one-third of the authorized toll charges. In the latest anti-fraud move, the FCC has now suggested that carriers rather than customers should be liable

for losses resulting from toll fraud. It has proposed that customers' liability should be limited and that there should be new equipment standards to make both PBX and mobile equipment more secure. PBX manufacturers say that customers should make use of safeguards already built into their systems before trying to shift responsibility.

WHAT YOU CAN DO NOW

While the arguments continue, customers should do their best to protect their systems:

- Change the system passwords once the equipment has been installed.
 - If you don't need the DISA feature, disable it.
 - Use a 'real time' monitoring system that can alert you to unusual activity. Some security companies now offer products that will create a profile of your normal telephone use and send out an alarm when there is a derivation from that profile.
 - Limit unsuccessful log on attempts to three tries.
 - Use a minimum of four digits in all passwords. Encourage employees to use as many as possible. An individual at the FCC hearing told me about 'War-dialers'. This is a program for cracking passwords that got its name from the movie, "War Games". A war dialer can crack an eight digit code in six hours. Obviously, being thrown out of the system after three unsuccessful attempts will slow down the thief. More digits will do the same.
 - Consider insurance. Prices can be reduced through discounts for safeguards or if other crime lines are purchased.
 - Read *Toll Fraud and Telabuse* for fraud prevention checklists and detailed case histories. It can be purchased from Telecommunications Advisors Inc., Portland, Oregon for about \$270.
 - Protect your RMATs. One security firm offers a call back modem that is programmed to accept calls only from a small list of numbers. When called, it disconnects and calls back authorized users only.
- Deactivate unused voice mail boxes. If you are going on an extended holiday, have someone monitor your voice mail. Thieves can take over a mailbox that has a message indicating the user is not available for an extended time.
 - Deactivate unused extensions.
 - Restrict access to problem area codes. Many companies block out area code 809 (The Caribbean). Approximately 60% of all PBX fraud calls terminate in the 809 area code. Others block out all international access codes. Keep in mind that Puerto Rico is not considered international so you will have to be specific. Emerging former East bloc countries are also a terminating point for many fraud calls. Consider your need to call these areas.
 - Limit trunk to trunk access on your systems. Some voice mail systems can give you an outside line.
 - Watch out for 'shoulder surfers' and be aware of your surroundings when you use an access code.
 - Utilize SMDR reports to detect unusual activity. Consider a security package that creates a user profile that will alert you to unusual activity.
 - Limit the capabilities of your system during non-business hours.
 - Make sure you have employee dishonesty insurance. An estimated 20% to 35% of fraudulent calls can be traced back to dishonest employees. Most of all, do not give up. The only thing limiting high-tech crooks is their imagination. Do not make it easy for them.

Frank Scheckton is
Senior Vice President of the
Fidelity & Crime Department at
Great American Insurance Company