another $11,500—to say nothing of the cost of registering PC Cyborg Corporation in Panama, or establishing an address in London. To add insult to injury, not one license payment was ever received from anyone, anywhere.

Popp's scheme was not particularly well thought out. The scam depended on recipients of his diskettes mailing checks halfway around the world in the hope of receiving an antidote to the trojan. But, as John Austen said, "Who in their right mind would send money to a post office box number in Panama City for an antidote that might never arrive?" Or that may not be an antidote anyway.

It seems unlikely that anyone will ever again attempt a mass blackmail of this type; it's not the sort of crime that lends itself to a high volume, low cost formula. It's far more likely that specific corporations will be singled out for targeted attacks. Individually, they are far more vulnerable to blackmail, particularly if the plotters are aided by an insider with knowledge of any loopholes. An added advantage for the perpetrators is the likely publicity blackout with which the corporate victim would immediately shroud the affair: every major corporation has its regular quota of threats, mostly empty, and a well-defined response strategy.

But at present, hacking—which gives access to information—has proven to be substantially more lucrative. Present-day hackers traffic in what the authorities call access device codes, the collective name for credit card numbers, telephone authorization codes, and computer passwords. They are defined as any card, code, account number, or "means of account access" that can be used to obtain money, goods, or services. In the United States the codes are traded through a number of telecom devices, principally voice-mail computers; internationally, they are swapped on hacker boards.

The existence of this international traffic has created what one press report referred to colorfully as "offshore data havens"—pirate boards where hackers from different countries convene to

trade Visa numbers for computer passwords, or American Express accounts for telephone codes. The passwords and telephone codes, the common currency of hacking, are traded to enable hackers to maintain their lifeline—the phone—and to break into computers. Credit card numbers are used more conventionally: to fraudulently acquire money, goods, and services.

The acquisition of stolen numbers by hacking into credit agency computers or by means as mundane as dumpster diving (scavenging rubbish in search of the carbons from credit card receipts) differs from ordinary theft. When a person is mugged, for example, he knows his cards have been stolen and cancels them. But if the numbers were acquired without the victim knowing about it, the cards generally remain "live" until the next bill is sent out, which could be a month away.

Live cards—ones that haven't been canceled and that still have some credit on them—are a valuable commodity in the computer underworld. Most obviously, they can be used to buy goods over the phone, with the purchases delivered to a temporary address or an abandoned house to which the hacker has access.

The extent of fraud of this sort is difficult to quantify. In April 1989 *Computerworld* magazine estimated that computer-related crime costs American companies as much as $555,464,000 each year, not including lost man-hours and computer downtime. The figure is global, in that it takes in everything: fraud, loss of data, theft of software, theft of telephone services, and so on. Though it's difficult to accept the number as anything more than a rough estimate, its apparent precision has given the figure a spurious legitimacy. The same number frequently appears in most surveys of computer crime in the United States and is even in many government documents. The blunt truth is that no one can be certain what computer fraud of any sort really costs. All anyone knows is that it occurs.

Leslie Lynne Doucette has been described as "the female Fagin" of the computer underworld. In her mid-thirties, she was consid-

(CONTINUED FROM FRONT FLAP)

erably older than the 150 or so adolescent Olivers she gathered into her ring. As a woman, she has the distinction of being one of only two or three female hackers who have ever come to the attention of the authorities.

In 1989 Doucette lived in an apartment on the north side of Chicago in the sort of neighborhood that had seen better days; the block looked substantial, though it was showing the first signs of neglect. Despite having what the police like to term "no visible means of support," Doucette was able to provide for herself and her two children, pay the rent, and keep up with the bills. Her small apartment was filled with electronic gear: personal computer equipment, modems, automatic dialers, and other telecom peripherals.

Doucette was a professional computer criminal. She operated a scheme dealing in stolen access codes: credit cards, telephone cards (from AT&T, MCI, Sprint, and ITT) as well as corporate PBX telephone access codes, computer passwords, and codes for voice-mail (VM) computers. She dealt mostly in MasterCard and Visa numbers, though occasionally in American Express too. Her job was to turn around live numbers as rapidly as possible. Using a network of teenage hackers throughout the country, she would receive credit card numbers taken from a variety of sources. She would then check them, either by hacking into any one of a number of credit card validation computers or, more often, by calling a "chat line" telephone number. If the chat line accepted the card as payment, it was live. She then grouped the cards by type, and called the numbers through to a "code line," a hijacked mailbox on a voice-mail computer.

Because Doucette turned the cards around quickly, checking their validity within hours of receiving their numbers and then, more importantly, getting the good numbers disseminated on a code line within days, they remained live for a longer period. It was a very efficiently run hacker service industry. To supplement her income, she would pass on card numbers to members of her ring in other cities, who would use them to buy Western Union money orders payable to one of Doucette's aliases. The cards were also used to pay for an unknown number of airline tickets and for hotel accommodation when Doucette or her accomplices were traveling.

The key to Doucette's business was communication—hence the emphasis on PBX and voice-mail computer access codes. The PBXs provided the means for communication; the voice-mail computers the location for code lines.

PBX is a customer-operated, computerized telephone system, providing both internal and external communication. One of its features is the Remote Access Unit (RAU), designed to permit legitimate users to call in from out of the office, often on a 1-800 number, and access a long-distance line after punching in a short code on the telephone keypad. The long-distance calls made in this way are then charged to the customer company. Less legitimate users—hackers, in other words—force access to the RAU by guessing the code. This is usually done by calling the system and trying different sequences of numbers on the keypad until stumbling on a code. The process is time-consuming, but hackers are a patient bunch.

The losses to a company whose PBX is compromised can be staggering. Some hackers are known to run what are known as "call-sell" operations: sidewalk or street-corner enterprises offering passersby cheap long-distance calls (both national and international) on a cellular or pay phone. The calls, of course, are routed through some company's PBX. In a recent case, a "call-sell" operator ran up $1.4 million in charges against one PBX owner over a four-day holiday period. (The rewards to "call-sell" merchants can be equally enormous: at $10 a call some operators working whole banks of pay phones are estimated by U.S. law enforcement agencies to have made as much as $10,000 a day.)

PBXs may have become the blue boxes for a new generation of phreakers, but voice-mail computers have taken over as hacker bulletin boards. The problem with the boards was that they became too well known: most were regularly monitored by law enforcement agencies. Among other things, the police recorded the numbers of access device codes trafficked on boards, and as the codes are useful only as long as they are live—usually the time between their first fraudulent use and the victim's first bill—the police monitoring served to invalidate them that much faster. Worse, from the point of view of hackers, the police then took steps to catch the individuals who had posted the codes.

The solution was to use voice mail. Voice-mail computers operate like highly sophisticated answering machines and are often attached to a company's toll-free 1-800 number. For users, voice-mail systems are much more flexible than answering machines: they can receive and store messages from callers, or route them from one box to another box on the system, or even send one single message to a preselected number of boxes. The functions are controlled by the appropriate numerical commands on a telephone keypad. Users can access their boxes and pick up their messages while they're away from the office by calling their 1-800 number, punching in the digits for their box, then pressing the keys for their private password. The system is just a simple computer, accessible by telephone and controllable by the phone keys.

But for hackers voice mail is made to order. The 1-800 numbers for voice-mail systems are easy enough to find; the tried-and-true methods of dumpster diving, social engineering, and war-dialing will almost always turn up a few usable targets. War-dialing has been simplified in the last decade with the advent of automatic dialers, programs which churn through hundreds of numbers, recording those that are answered by machines or computers. The process is still inelegant, but it works.

After identifying a suitable 1-800 number, hackers break into the system to take over a box or, better, a series of boxes. Security is often lax on voice-mail computers, with box numbers and passwords ridiculously easy to guess by an experienced hacker. One of the methods has become known as finger hacking: punching away on the telephone keypad trying groups of numbers until a box and the appropriate password are found. Ideally, hackers look for unused boxes. That way they can assign their own passwords and are less likely to be detected. Failing that, though, they will simply annex an assigned box, changing the password to lock out the real user.

VM boxes are more secure than hacker boards: the police, for a start, can't routinely monitor voice-mail systems as they can boards, while hackers can quickly move to new systems if they suspect the authorities of monitoring one they are using. The messaging technology of voice-mail systems lends itself to passing on lists of codes. The code line is often the greeting message of the hacker-controlled mailbox; in other words, instead of hearing the standard "Hello, Mr. Smith is not in the office. Please leave a message," hackers calling in will hear the current list of stolen code numbers. In this manner, only the hacker leaving the codes need know the box password. The other hackers, those picking up the codes or leaving a message, only need to know the box number.

It was ultimately a voice-mail computer that led the authorities to Doucette. On February 9, 1989, the president of a real estate company in Rolling Meadow, Illinois, contacted the U.S. Secret Service office in Chicago. His voice-mail computer, he complained, had been overrun by hackers.

The harassed real estate man became known as Source 1. On February 15th, two Secret Service agents—William "Fred" Moore and Bill Tebbe—drove from Chicago to the realtor's office to interview him. They found a man beset by unwanted intruders.

The company had installed its voice-mail system in the autumn of 1988. The box numbers and passwords were personally assigned by the company president. While the 1-800 number to access the system was published, he insisted that the passwords were known only to himself and to the individual box users.

In November 1988, during an ordinary review of the traffic on the system, he had been startled to discover a number of unexplained messages. He had no idea what they were about or who they were for; he thought they could have been left in error.

However, the number of "errors" had grown throughout November and December. By January 1989 the "errors" had become so frequent that they overwhelmed the system, taking over almost all of the voice-mail computer's memory and wiping out messages for the company's business.

The Secret Service recorded the messages over a period from late February to March. Listening to the tapes, they realized they were dealing with a code line.

The law on access devices prohibits the unauthorized possession of fifteen or more of such codes, or the swapping or sale of the codes "with an intent to defraud." (Fraud is defined as a $1,000 loss to the victim or profit to the violator.) On the tapes, the agents could identify 130 devices that were trafficked by the various unknown callers. They also heard the voice of a woman who identified herself alternatively as "Kyrie" or "long-distance information." It seemed as if she was running the code line, so they decided to focus the investigation on her.

In March security officials from MCI, the long-distance telephone company, told the Secret Service that Canadian Bell believed "Kyrie" to be an alias of Leslie Lynne Doucette, a Canadian citizen who had been hacking for six or seven years. In March 1987 Doucette had been convicted of telecommunications fraud in Canada and sentenced to ninety days' imprisonment with two years' probation. She had been charged with running a code line and trafficking stolen access codes. Subsequently, the Canadians reported, Doucette had left the country with her two children.

Later that month an MCI operative, Tom Schutz, told Moore that an informant had passed on the word that a well-known hacker named Kyrie had just moved from the West Coast to the Chicago area. The informant, Schutz said, had overheard the information on a hacker "bridge" (a conference call). At the beginning of April an MCI security officer, Sue Walsh, received information from another informant that Kyrie had a Chicago telephone number.

By mid-month, Moore was able to get court authorization to attach a dialed-number recorder (DNR), to Doucette's phone. A DNR monitors outgoing calls, recording the number accessed and any codes used. From the surveillance, agents were able to detect a large volume of calls to various voice-mail systems and PBX networks.

The authorities traced the other compromised voice-mail systems to Long Beach, California, and Mobile, Alabama. They discovered that Kyrie was operating code lines on both networks. It's not unusual for hackers to work more than one system; sometimes Hacker A will leave codes for Hacker B on a voice-mail computer in, say, Florida, while Hacker B might leave his messages for Hacker A on a system in New York. By rotating through voice-mail computers in different states, hackers ensure that local law enforcement officials who stumble upon their activities see only part of the picture.

The agents also realized that Kyrie was running a gang. From other sources they heard tapes on which she gave tutorials to neophyte hackers on the techniques of credit card fraud. Over the period of the investigation they identified 152 separate contacts from all over the country, all used as sources for stolen codes. Of the gang, the agents noted seven in particular, whom they identified as "major hackers" within the ring: Little Silence in Los Angeles; the ironically named FBI Agent in Michigan; Outsider, also in Michigan; Stingray from Massachusetts; EG in Columbus, Ohio; Navoronne, also from Columbus; and Game Warden in Georgia.[4] DNRs were also attached to their telephones.

The agents assigned to the case described the group, imaginatively, as "a high-tech street gang." By then the Secret Service had turned the enquiry into a nationwide investigation involving the FBI, the Illinois State Police, the Arizona Attorney General's Office, the Chicago Police Department, the Columbus (Ohio) Police Department, the Cobb County (Georgia) Sheriff's Office, the Royal Canadian Mounted Police, and the Ontario Provincial Police. Security agents from MCI, Sprint, AT&T, and nine Bell phone companies provided technical assistance.

On May 24th the Secret Service asked local authorities in six cities for assistance to mount raids on Doucette's Chicago apartment and the addresses of the five other major hackers in the ring. Prior to the raids the authorities compiled a list of equipment that was to be seized: telephones and speed-dialing devices; computers and peripherals; diskettes; cassette tapes; videotapes; records and documents; computer or data-processing literature; bills, letters, invoices, or any other material relating to occupancy; information pertaining to access device codes; and "degaussing" equipment.[5]

The raid on Doucette's Chicago apartment produced a lode of access codes. Moore found a book listing the numbers for 171 AT&T, ITT, and other telephone cards, as well as authorization codes for 39 PBXs. In addition, the agents found numbers for 118 Visa cards, 150 MasterCards, and 2 American Express cards.

Doucette admitted that she was Kyrie. Later in the Secret Service offices, she confessed to operating code lines, trafficking stolen numbers, and receiving unauthorized Western Union money orders. She was held in custody without bond and indicted on seventeen counts of violating federal computer, access device, and telecom fraud laws between January 1988 and May 1989.

Estimates of the costs of Doucette's activities varied. On the day of her arrest, she was accused of causing "$200,000 in losses . . . by corporations and telephone service providers." Later it was announced that "substantially more than $1.6 million in losses were suffered" by credit card companies and telephone carriers.

Doucette's was a high-profile arrest, the first federal prosecution for hacking voice-mail systems and trafficking in access devices. The prosecution was determined that she would be made an example of; her case, the authorities said, would reflect "a new reality for hackers" in the 1990s—the certainty of "meaningful punishment." If convicted of all charges, Doucette faced eighty-nine years' imprisonment, a $69,000 fine, and $1.6 million in restitution charges.

The case was plea-bargained. Doucette admitted to one count; the other charges were dismissed. On August 17, 1990, Doucette, then aged thirty-six, was sentenced to twenty-seven months in prison. It was one of the most severe sentences ever given to a computer hacker in the United States.[6]

Willie Sutton, a U.S. gangster, was once asked why he robbed banks. "Because that's where the money is," he replied.

Little has changed; banks still have the money. Only the means of robbing them have become more numerous. Modern banks are dependent on computer technology, creating new opportunities for fraud and high-tech bank robbery.

Probably the best-known story about modern-day bank fraud involves the computation of "rounded-off" interest payments. A bank employee noticed that the quarterly interest payments on the millions of savings accounts held by the bank were worked out to four decimal points, then rounded up or down. Anything above .0075 of a dollar was rounded up to the next penny and paid to the customer; anything below that was rounded down and kept by the bank. In other words, anything up to three quarters of a cent in earned interest on millions of accounts was going back into the bank's coffers.

Interest earned by bank customers was calculated and credited by computer. So it would be a simple matter for an employee to write a program amending the process: instead of the rounded-down interest going back to the bank, it could all be amalgamated in one account, to which the employee alone had access. Over the two or three years that such a scam was said to have been operational, an employee was supposed to have grossed millions, even billions, of dollars.

The story is an urban legend that has been told for years and accepted by many, but there has not been a single documented case. However, it certainly could be true: banks' dependence on computers has made fraud easier to commit and harder to detect. Computers are impersonal, their procedures faster and more anonymous than paper-based transactions. They can move