Portrait of the Computer Criminal

J.M. Carroll, Department of Computer Science, University of Western Ontario, London, Canada

This paper assesses the past, present and future of computer crime -- from its origins a quarter century ago when dissident students bombed and burned computers, while greedy programmers altered programs so their checking accounts would be forever full; to the present day when the massive Internet is so thoroughly penetrated that no user can rely on the integrity of data. It presents the computer as the victim, environment and tool of the criminal. Then it characterizes the computer criminal and explores his/her motivation, opportunities, means and methods.

1. COMPUTERS AND CRIME

In the 21th century almost all crime against property will be perpetrated within computer systems. Furthermore, many other crimes, even violent ones, will be controlled or directed by computers. The principal reason for this will be the central role played by computer systems in storing and processing the assets of individuals and organizations, and in directing the activities of enterprises.

There are two secondary reasons. First, the computer industry has expanded and prospered by emphasizing speed, efficiency and product versatility. The tasks of maintaining the confidentiality and integrity of the information processed by computer systems has been a secondary consideration.

Secondly, persons responsible for writing, enforcing and interpreting the law have failed to grasp the full import of the cybernetic revolution and have striven valiantly but, for the most part, ineffectually to force computer technology into pigeon holes that were designed for quill pens and parchment. Even the phrase "computer crime" is a misnomer. Computers do not commit crimes any more than firearms kill people. People commit all the crimes.

Computer crime is difficult to prosecute because offenders sometimes know a great deal more about computer technology than do prosecutors and judges. To cope with computer crime, you must understand how computer criminals work and what legal and technological weapons can be used against them.

The computer can be the object of crime, a tool of crime, and it can provide the environment within which crime can prosper. It was as an object of crime that the computer first achieved public notoriety.

1.1. The Computer as an Object of Crime

By the mid-1960's computers were already performing repetitive, and formerly people-intensive, tasks for many large organizations. They recorded student grades and mailed out grade reports, posted bank checks, calculated payrolls and printed pay checks. The typical computer system occupied a single large room filled by massive racks of electronic equipment. Adjoining the computer center were rooms devoted to electro-mechanical equipment used by clerks who converted documents into decks of punched cards that were then fed into to the computer.

A computer was a status symbol for the organization that owned one. One side of the computer room was a huge plate-glass window. On-lookers gathered before it as if to do homage to a new deity. They marvelled at the blinking multi-colored lights and whirling magnetic tape drives. Men leered as a bevy of stylishly dressed young women threw switches, pushed buttons, carried in boxes punched cards, and carried out reams of print-out.

Burning Down the Computer. But the nineteen sixties were revolutionary times. Young people were angry. They rebelled against an older generation that killed their heroes, abhorred their music, jailed them for smoking marijuana, told them whom to hate, and sent them to die in a far-away jungle. To these angry young people, the computer was a symbol of all they thought was wrong with the Western world.

The angry young people smashed the plate-glass windows and trashed the electronic behemoth. At Boston University they attacked it with wire cutters and doused it with acid. At Fresno State and New York University, they threw fire bombs at it. At the University of Wisconsin in Madison and at the University of California in Berkeley they blew it up with dynamite.

At Sir George Williams University in Montreal, now part of Concordia, dissident students celebrated the dawn of the 1970s by breaking into the computer center. For the next 42 days they occupied the center. Holding the vital computer hostage, they taunted the administration, brought registration for the new semester to a stand-still, and from time to time showered boxes full of computer cards and streamers of magnetic tape down on Maisonneuve Blvd. There were ugly racial overtones to the occupation. Most of the student were from Caribbean islands and one told reporters that a reason for the occupation was because a biology professor had vowed never to give a black student a grade higher than "C".

On February 11, 1970, Montreal riot police stormed up the central staircase of the building towards the computer center. The students made good a threat to destroy the computer. They torched a mountain of spoiled print-out and carry-out food containers and set the computer center on fire. The demonstration ended as the \$1.6-million computer was immolated under a shroud of acrid smoke

and tear gas. As a sidelight on the Sir George Williams case: the leader of the dissidents, Roosevelt "Rosie" Douglas, was deported to his native island of Dominica where he became leader of the opposition Labor Party. A female accomplice was appointed to the Senate of Canada.

Birth of the Hacker. From the ashes of Montreal and the rubble of Madison and Berkeley there sprang a new profession, Computer Security. The era of the show-cased corporate computer passed into history. Computer centers were turned into well-hidden fortresses and their critical back-up information was sequestered in off-site bank vaults.

But business needs ready access to its computer-stored information and during the decade of the seventies on-line remote-access became the method of choice for communicating with the main-frame computer hidden away, secure within its magic mountain. Video display terminals that looked like over-grown television sets and printing terminals that looked like elaborated electric typewriters became commonplace. They were "dumb" terminals, however, utterly dependent upon hundreds of umbilical cords linking each one to the far-away main-frame computer.

Few thieves were attracted to dumb terminals because without their umbilical cords they were useless. The main threat to security was, and remains, an attack of the computer's communications network. No longer did an unauthorized user have to submit a card deck at a service counter within a secure area and return later to retrieve the print-out, all the time risking being identified and taken into custody. A new species of low-life had mutated -- the hacker was born. The objective of the hacker was, and is to steal computing service and the information stored within the computer's memory.

1.2. Stealing the Computer

The decade of the 1980s saw the personal computer eclipse the giant main-frame for all but the most intensive computational applications -- like producing realistic special effects for feature motion pictures. The PC puts on anyone's desk more than 100,000 times the computing power of a circa 1970 main-frame. Moreover, as these PCs replaced the dumb terminals, they became nodes in vast computer networks in which the main-frame itself is replaced by an enhanced PC called a client server.

The PC of the 1990s has become a common-place appliance in many homes and an extension of the workplace. The desk-top computer has been shrunk for people who want to take it with them on the road. It no longer need be a desk-top. It can be a lap-top. And there are even smaller versions that can be carried and used on jobs such as land surveying or taking inventory. These are called palm-top computers.

Personal computers of all sizes have become prey to the same

kind of marauders who steal stereos and television sets, with an important difference. Even the smallest PC can contain a hard-disk memory capable of holding more than 100 million or more characters of information. Therefore, the thief who steals even a lap-top computer could be stealing the victim's library as well. Indeed, a thief in England stole a lap-top computer from the automobile of a military staff officer. The computer's memory contained the detailed plans for Great Britain's participation in the Gulf War.

Once again the computer has become the object of crime. Today, the adversary is not the would-be revolutionary attacking what is perceived as a symbol of established power. Today the motive is not political destabilization but theft of valuable consideration; and the potential perpetrators are far more numerous. They range all the way from the local house-breaker to the industrial spy or hostile secret agent. Educational PCs especially like to "grow legs" and walk away. Insurance companies are threatening to cancel burglary policies of universities unless burglar bars are installed on first-floor windows of computer labs and campus police are able to demonstrate five-minute response to power-cord alarms.

1.3. The Computer as a Tool of Crime

Criminal enterprises have made use of high-speed automobiles, specially designed "cigarette" boats, aircraft, radio communications, steel-burning lances, and cryptographic devices; so why not computers?

Managing Criminal Enterprises. Computer scientists not infrequently are asked to help police in situations where a criminal entrepreneur has made use of a computer to further some criminal intent or to impede a police investigation. A California sheriff had arrested a former computer programmer who was alleged to be the operating mind behind eleven underground cocaine laboratories as well as dealing in automatic firearms, military explosive devices, and undertaking contract murders.

Incident to the suspect's arrest, deputies had seized a personal computer with a 40-million byte (character) hard-disk memory. All the data on the disk was encrypted except the one file the suspect was working on when he was apprehended. The contents of this clear-text file suggested that the encrypted files might contain the locations to the suspect's factories and storage locations, names of criminal associates, and inventories of contraband material. The sheriff wanted help to decrypt the disk.

The encryption system was a commercially available version of the U.S. government's Data Encryption Standard, realized in a combination of hardware and software. Discussions with the manufacturer suggested that it would not be feasible to decrypt the files by cryptanalysis. An attempt was made to recover the eight-byte key to the cipher by calling the suspect's former employers in California's Silicon Valley and asking them to help prepare a list of the passwords the suspect had used while in their employ, on the

chance that he may have used one of them as the key to the cipher.

The investigation terminated, however, when the Federal Bureau of Investigation entered the case. They had a warrant charging the suspect with interstate flight to avoid prosecution for murder, which took precedence over the California drug charges. He was wanted for the murder of two Colorado businessmen who died when one of them turned the ignition key of the car they were sitting in and triggered a bomb hidden beneath the floor boards.

Facilitating Illegal Acts. In another case, a computer systems manager was approached by a detective of the Ontario (Canada) Provincial Police to help in an investigation of an illegal pyramid scheme. Police had seized from a suspect a computer that contained apparently encrypted files on its hard disk. They were thought to be relevant to the case. The manager recognized that the files were encrypted in a cipher used by a popular word processing program to "lock" files. The encipherment was reversed using an access code already available to the investigator. Thereupon the entire tree structure of the pyramid scheme was revealed together with names, addresses and the monetary value of each participant's contribution. This evidence helped to convict the ring-leader of offenses under s. 206 of the *Criminal Code*¹ (lotteries and games of chance).

Other criminal endeavors assisted by computers include: preparing and mailing false invoices with the expectation that business people will be duped into paying them, maintaining inventories of child pornography photographs and videos, calculating odds and lay-offs for bookmakers, and keeping records of cannabis smuggling. There is even a case in which a serial rapist-killer made use of a computerized dating service to select and meet his victims. In one case currently under investigation, police arrested a homosexual pedophile who was recruiting 13-14 year-old boys through a "Gay" Bulletin Board on Internet. These boys, in turn, recruited younger boys, many of whom dropped out of sight after making a contact. At last reports, police, with German shepherd dogs, were digging up a considerable amount of real estate around the suspect's home.

Any criminal enterprise with a business flavor can profit from computer assistance. Even armed robbers could use a simple simulation program to target variety stores randomly so as to avoid using a selection pattern that would make it easy for police to stake-out probable crime sites.

1.4. The Computer as an Environment for Crime

Since 1966 when Milo Arthur Bennett, computer programmer for a Minneapolis insurance company, which was reconciling checks for the National City Bank of Minneapolis, arranged for its computer not to post his personal checks, computers have been a rich environment in which to perpetrate all manner of fraud. Bennett confessed to his fraud, was placed on probation and made

restitution of the \$1,357 he stole.

The Era of Forgiveness. The years prior to 1974 were an era of forgiveness for computer criminals. Youthful "hackers" who broke into computer systems were regarded as budding geniuses and were punished only by having to write essays on how they did it. They included the MIT students who in 1967 discovered an unused data line into the Strategic Air Force computer in Omaha. They used it to access SAC's computer and leave indications of their presence. This greatly perturbed the Air Force generals and provided the models for the motion picture "War Games".

The universities were veritable play pens of computer crime. At the University of Western Ontario, a student logged in on two terminals at one time. One terminal was programmed to continually issue the command "Attach Job Number 1". Using the other terminal, the student obscenely harassed the system operator. When she dropped her job to kill his, his other terminal immediately became attached to her job (Job No. 1), making the student the systems operator. He then sent to all 200 terminals the message "The system is mine!"

At the University of Waterloo, at least one computer science professor announced a standing offer to buy a pitcher of beer for any student who was able to break into the university computer system, reputed to then be one of the most secure in the world. That is, without authorization the student would have to upgrade his privilege to equal that of a system manager. One of the winning submissions, called by some the "Misguided Missile", was a prototypical synchronous attack (infra).

Even hackers who took value in their trespasses, such as Jerry Schneider who defrauded Pacific Bell Telephone of \$2 million, and Ian Murphy who defrauded Pennsylvania Bell out of toll charges for himself and friends, were treated leniently. Schneider and Murphy went on to become computer security consultants. Schneider had learned how to activate the telephone company's inventory ordering system and direct that material be delivered to notional job sites throughout Los Angeles. Before day-break, Schneider collected the stashes of cables and hardware in his surplus telephone company van and took them to his warehouse from whence he sold them; sometimes right back to Pacific Bell. As a rule, offenders were either not prosecuted, or they readily confessed to any kind of misdemeanor charge the prosecutor chose to lay, secure in the knowledge that the severest punishment they would get would be probation. Schneider got 49 days in jail and had a restitution order entered against him for \$141 a month.

Criminalizing Computer Crime. By the mid-1970s the cost of computer crime began to tarnish the perceived brilliance of the perpetrators and society recognized computer criminals for the thieves and mischief-makers they were. Initially the courts tried to bring computer-related offenses into the ambit of conventional crime laws. Sometimes they succeeded. In 1974 at least three criminal

groups conspired to defraud the Canadian Unemployment Insurance system. They created notional individuals with false Social Insurance numbers; one group even created a notional company that laid off their notional employees. The other groups were content with forging individual documentation. Ring members working as UI claims supervisors approved bogus claims; co-conspirators picked up the UI checks and cashed them.

An RCMP sergeant broke the case when he had the UIC sort recent UI claims by address. He noticed that many recipients "lived" in one Montreal apartment complex, as many as 12 to an apartment. On pokey day, mounties staked out the apartment house and identified a young couple following the postman around and collecting UI checks from mailboxes. They were arrested and found to be in possession of 36 SIN cards matching the checks they had picked up. Tellers in various suburban banks identified the woman as having previously cashed UI checks like those in her possession. The woman was a UI claims supervisor; the man was her live-in boy friend. He was legitimately unemployed. The offenders were each charged under the *Criminal Code* with 36 counts of obtaining money under false pretences contrary to ss. 362(1); 36 counts of uttering false documents contrary to ss. 368(1)(b); and one count of conspiracy to commit an indictable offence contrary to ss. 465(1)(c). They were successfully prosecuted.

2. THE ANATOMY OF COMPUTER CRIME

The steps in the analysis of any crime are delineated in the acronym: MOMM². It stands for Motive, Opportunity, Means, and Method.

2.1. Motivation.

The Motives for computer crime are delineated by a second acronym: MICE². It stands for Money, Ideology, Compromise, and Egotism.

Money. At least half a dozen or more classes of computer criminal are motivated by the fraudulent pursuit of money:

1. Authorized person with custody of enterprise funds who unlawfully converts them to his own use -- the embezzler. The embezzler is usually a middle-aged white male occupying a position of trust who has reached the pinnacle of his career and is beset with an unsharable need for cash because of family illness, children's education, unwise investments, or extra marital affairs.

2. Data diddler. This person is usually a female, 25-35 years old, frequently a member of a minority group, who is employed as a data input supervisor. If she is a bank teller, she extracts money from the system by unlawfully transferring customer deposits to a co-conspirator's account. If she is a benefits supervisor, she approves false claims on behalf of friends and shares the proceeds with them.

3. "Real" computer criminal is usually a thirty-something male of any racial or ethnic background, employed as a computer programmer, systems manager or center director. He knows how to bypass system security and accounting controls. He can operate his own business using his employer's facilities, steal trade secrets and sell them to competitors, and revise application programs so they carry out elaborate frauds that payoff to him for years to come.

4. Hacker. Usually the hacker breaks into computer systems for the fun of it. Increasingly, hackers are doing it for profit as well as pleasure. A ring of West German hackers sold industrial and military secrets to the then East German state. More recently, hackers have been providing cheap long-distance phone service on an underground market, having acquired access codes by break-ins.

5. The Sorehead. This person has lost out on a promotion he or she coveted, been "red-lined" for layoff, or is simply angry at the "boss". The sorehead uses all the access he was given legitimately or has gained by experimenting with the system or observing other workers to wreck havoc with the system. Soreheads will erase files or scramble them. It is difficult to meet the criminal standard of proof beyond a reasonable doubt when prosecuting them because it is hard to tell malice from simple negligence. The way to handle this creature is to have a regular back-up system in place, and after you fire him/her, sue civilly for the time and trouble these actions cost. In civil court, the standard of proof is the balance of probabilities and negligence can be actionable. There are lots of soreheads around in these days of restraint and down-sizing.

6. The "Midnight Entrepreneur". This fellow is running his own business using the boss' hardware, software and customer lists. There are a number of actions open to the aggrieved employer: breach of contract, confidentiality or fiduciary duty. The employer can not only recover the faithless employee's profits but any of his real or personal property into which profits can be traced.

Ideology. Ideological criminals include demonstrators who destroy computers for political reasons, data diddlers who help finance revolutionary causes, union members identified as essential (i.e. prohibited by law from striking) who purposefully cause systems to "crash" during a strike, and discharged or disgruntled computer operators who erase or randomly scramble files to exact revenge on their employers or former employers.

Compromise. Persons who commit crimes because of compromise include females in abusive relationships who cause computers to issue fraudulent checks in favor of their partners; or persons who are blackmailed into revealing passwords and access codes to potential system infiltrators. Their unlawful acts may be a way of paying gambling debts or "vigorish" on a usurious loan from an organized crime figure; or married persons enticed into illicit relationships.

Egotism. The fourth class of computer criminal includes the majority of hackers and virus writers. They break into computer systems or sabotage their operations principally to confound legitimate computer users. Their depredations are acts of supreme egotism. They are sending out the message: "I am smarter than anybody. So there!" The egotist is usually a white male aged anywhere from eight to 25 years.

2.2 Opportunity to Commit Computer Crime

Opportunity equates to knowledge and access. The knowledge can encompass any or all of the following: communications protocols, application programs, computer operating systems, database and file management systems, and accounting procedures. Access can be either physical or electrical. Anyone who can physically take over a computer console or keyboard; submit a job at a service counter for processing; execute a program; use a text editor; provide a software package; dial into an on-line system; or even send someone an electronic mail message, can, if he or she knows enough about the target system, access it, acquire its highest level of privilege, and obtain whatever benefit, privilege, commercial advantage, or valuable consideration the system is able to confer.

2.3 Means of Commission

A computer crime begins with the perpetrator gaining unauthorized access to the target computer system; or if the intruder already has some level of authorized access, exceeding it so as to be privileged to realize his criminal purpose. That purpose may be:

1. Further an intent to fraudulently obtain value. This usually means getting the computer to issue a check to the intruder or a co-conspirator; or to transfer assets to a place under the intruder's control.

2. Read or copy confidential or other kinds of protected information. These could include military, diplomatic, financial, law enforcement, or medical data; or trade secrets.

3. Insert or alter programs or data so to confer a benefit, privilege, pecuniary advantage or valuable consideration on the intruder or a co-conspirator. Examples include unauthorized changes to payrolls, accounts payable, accounts receivable, or inventory accounts.

4. Impede or obstruct operations of legitimate users by damaging the reliability of hardware or software; or reducing the usefulness or effectiveness of data.

2.4 Methods of the Computer Criminal

There are four steps in committing a computer crime:

1. Obtain access to the computer system.
2. Extend access until the criminal intent can be realized.
3. Scrutinize, modify, defraud, or destroy information.
4. Remove evidence of unauthorized entry.

The most important step is gaining access. Access to a computer system, program or database is controlled by making users identify themselves and then authenticate their identity. Authentication can be accomplished by testing knowledge of a password, possession of an artifact, or having some biological or behavioral characteristic. Any of these mechanisms can be defeated. Access control by use of an automatic fingerprint reader was thought to be invincible until a terrorist group kidnapped a bank manager and cut off his right thumb to activate a critical access control system. Actually the password is still by far the most used means of authentication.

*Obtaining Access*³. The methods of the computer criminal have spawned a glossary of colorful terms:

Masquerading is the general term for gaining access by assuming a legitimate user's identity and authentication. It can be accomplished by interception, misappropriation, or forgery of the user's authenticating credentials, usually a password. Specific techniques include:

Scanning, obtaining a dial-in computer's unpublished telephone number by using a PC to scan an entire exchange of 10,000 numbers.

Wiretapping data lines leading to the computer to capture passwords when transmitted by or echoed to legitimate users.

Shoulder Surfing, penetrating a computer center or terminal area and observing passwords that may be taped to display screens. A typical disguise is as a pizza delivery person.

Optical spying, observing from a nearby building with a high-powered telescope.

Eavesdropping, attaching "bugs", clandestine radio transmitters (or any electro-magnetic, acoustic or mechanical device) to data lines (or busses, power lines, or structural members) within the center. The signals intercepted can be displayed on a Data Line Monitor. Disguise as a telephone company repairman to plant the "bug".

Intercepting free-space electro-magnetic emanations (Minispy) from monitor screens. This is called a Tempest interception. The FBI may have used this device to gather evidence of the alleged spying of Rick Ames on his employers in the CIA.

Scavenging, reading discarded print-out in trash bins.

Simulation, programming a computer to imitate the target computer and using it to collect passwords of users who dial into it. Can be implemented by surreptitious Call Forwarding.

Deception, Calling the Security Officer to say: "I am Joe Big-Shot and I forgot my password."

Corruption, bribing or compromising a legitimate user.

Guessing, or using an off-line Password Breaker that matches a lexicon of more than 10,000 possible passwords against an encrypted list stored within a computer running under the Unix operating system (Most operating systems do not even bother encrypting the password list.).

Entry can also be gained by following an authorized user who has left the computer in an insecure state. These attacks are called:

Object Reuse, in which the work of a prior user of a time sharing computer system can become available to the next user.

Piggybacking, in which an unauthorized user takes over an active job left alive by a previous legitimate user.

Tailgating, refers to gaining physical access by closely following an authorized user through a turnstile or man-trap.

Between-the-Lines Entry, taking over a logged in terminal or PC when the authorized user goes to lunch or the washroom.

Extending Authority. Extending entrance-level authority usually requires detailed knowledge of the computer's operating system. Users can extend their authority by:

Browsing, observing the contents of publicly available directories for clues as to what the computer is used for.

Covert Channels, observing the usage of computer memory and any increase in operating-system response time to user requests to determine what programs are executing.

Trap Doors, making use of paths that by-pass security controls and were left in the system from its developmental period.

Back Doors, by-pass programs inserted by intruders that permit re-entry to the intruder upon typing a password known only to him.

Superzapping, using utility programs that violate security controls to allow making run-time alterations to programs and data, to accomplish an unlawful purpose.

Superuser, also called a Root Attack. Using commands of the popular Unix operating system to deceive the computer into accepting an intruder as the system manager (known as the Superuser). Requires use of a Superzap.

Synchronous Attacks, misdirecting sub-routine calls to put the computer in a privileged mode of operation.

Scrutinizing, Changing or Destroying. Having gained access to the source code of an accounting program, a criminal with programming skills can modify the programs to steal small amounts from a large number of accounts by Salami or Round-off attacks. The perpetrator may store these amounts in his income tax withholding account so he gets his ill-gotten gains in the form of a large tax refund.

The Trojan Horse is a malicious program that resembles a legitimate one but does something unexpected when activated, like giving its writer unlimited authority over the system (e.g. a Back Door). Trojan Horses can be infiltrated by electronic mail.

Computer Virus is a kind of Trojan Horse that can attach itself to other programs so that they also become viruses.

Worm is a kind of virus that endlessly replicates itself until it consumes all the memory a computer has and causes it to "crash" or become inoperable.

Logic Bomb is a malicious program (often a Trojan Horse) that rests dormant until triggered by some event such as the occurrence of a predetermined calendar date and time.

Stealth Program, frequently a virus, can hide itself somewhere in the dark recesses of the computer's massive memory, sometimes in encrypted form. It will remain dormant until awakened by its creator re-entering through a Back Door, by some user deceived by a Trojan Horse, or by the detonation of a Logic Bomb.

The complex frauds that can be accomplished by manipulating computer programs have as their ultimate objective getting an enterprise computer to produce a check drawn in favor of the perpetrator or an accomplice; or in a bank fraud, transferring money into a demand account controlled by the perpetrator.

A common ploy is to establish a notional company, get it qualified as a vendor to the target company for some product or service not subject to inventory or other audit control: consulting services, computer programming, linen supply, trash removal, foundry sand, and supplies for cleaning and maintenance have all been used successfully. Then regularly enter bogus invoices into the accounts payable system and there after manage the fictitious company in the offender's home computer, being sure to file and remit corporate income tax.

Erasing the Evidence. Any intruder who is able to extend

unauthorized access to get into a protected machine state can alter the audit trail. This is a continuous log kept by the computer as a record of who enters at what date and time. It may also record what programs were executed and which files were changed. However, a skillful intruder can alter the log to remove all trace of entry, and even to "frame" some legitimate user. As long as such weaknesses exist in the security posture of computers, attribution of computer crime to any but the most unsophisticated offenders is all but impossible.

2.5 Computer Crime Today

Internet is a computer network of 21,000 networks connecting two million computers. It serves 15 million users in 60 countries and it is growing at an annual rate of 7 to 10 percent.

On February 3, 1994 the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, an activity sponsored by the U.S. Department of Defense, flashed a warning over Internet: "Systems of some service providers have been compromised. Intruders have captured access to information for tens of thousands of computers across Internet."⁴

On February 11, a European security group with close ties to Interpol, transmitted a restricted distribution advisory that the intruders had launched a Virus that makes a Root Attach on Unix operating systems and establishes Back Doors that allow the intruders to enter the computer at any time. These events suggest that nobody's computer-stored information may be safe or reliable any more.

In the war against computer crime, what goes around comes around. In hard times, computers are attacked by the losers of this world. In fat times they become the tools of the "get rich quick" schemers. The computer criminal is a person for all seasons; a person keen to exploit every technical advance before its originators have wrung their first profit from it.

REFERENCES

1. *Criminal Code*, Revised Statutes of Canada 1985, c. C-34.
2. Jack Bologna, *Computer Crime: Wave of the Future, Assets Protection*, San Francisco, 1981.
3. John M. Carroll, *Computer Security* c. 2 (1977, 1987, 1995 [in preparation]).
4. *Computerworld*, February 14, 1994, p. 14.