LET'S CRACK DOWN ON HACKERS

Fred Benner

(1) Sitting in front of his home computer console, a teenage boy feverishly types in password after password in an attempt to access the mystery computer he has stumbled upon. Although he is somewhat discouraged by his vain attempts to solve this particular Rubik's cube, he finally cracks the code and he is "in." Like a kid in a candy store, he excitedly applies his small amount of knowledge of computers obtained through a summer course and "browses" through the system. After a thorough look, he hangs up the phone, finishes his algebra homework, and goes to bed, satisfied with his computer safecracking achievement.

(2) Does this sound like a scene from the popular movie, War Games? As impossible as it seems, our mental image of the computer "hacker" (so-named for the ability to hack-up computer systems) is not so far from reality, but not as glamorous as it looks. Hacking should be recognized as nothing more than what it really is--breaking and entering, invasion of privacy, and in some cases, theft and destruction of property. It should also show why there is a need for government regulation of home computers.

(3) Hacking is a fairly simple and relatively inexpensive "hobby" which doesn't require a great deal of computer knowledge. The tools of the trade are nearly any home computer and a device called a modem which is used to translate the computer's "language" and allow the computer to talk over the phone lines. Now all the hacker needs is information to break in to other systems. This information is readily available through dial-up computerized bulletin boards such as "cracker" bulletin boards. These boards are run by such underground groups as "T.H.E.M." (Telecommunications Hackers, Embezzlers, and Manipulators) (Gillard and Smith 406). Many such boards provide information on obtaining free long-distance services such as "Sprint" and "MCI" and how to prevent such illegal calls from being traced (Marback et al. 43).

(4) Computer crimes range from the small-time kid's break-in to large-scale crimes such as theft and embezzlement. In some cases ex-employees use the computer to seek revenge on their former employers. One such case occurred when a programmer was fired from his job at a software firm. To gain revenge, he broke in to the company's computer using another employee's password and learned confidential software secrets. He then marketed his own similar software at cheaper prices to take business away from his former employer (Gillard and Smith 398).

(5) Such criminals are almost impossible to detect since computers retain little or no trace of their break-in. Even

when the crime is detected, the person who committed the crime is long gone. Estimates of losses due to computer crimes are difficult to obtain since those hardest hit are banks and small businesses which would be less likely to report such crimes for fear of losing the trust and business of their customers and shareholders (Halper 61). Most losses are simply written off as business expenses and passed along to the consumer. But is it fair that we pay the price just because some thief was "joyriding" through our bank accounts?

(6) Another expense which is passed along to the consumer is the high cost of computer security. Several methods of computer security are in use today, all of them very costly. In one method, called encoding, a "black box" is placed at the main computer and at all the branch computers. The boxes scramble all data transferred so that anybody without an encoding device will not be able to decipher what is going on (Marback et al. 46). Another method uses a call-back device whereby the user calls the main computer and types in his phone number; the computer then hangs up, checks its file for authorized user phone numbers, and calls the user back if his number is approved (Marback et al. 46).

(7) Other simpler methods of security are (1) regular changes of entry passwords, (2) requiring employee I.D. number and birthday, (3) limiting the number of allowable attempts to enter, or (4) keeping a record of user activity on the system to see who is trying to enter confidential files ("Computer Security" 127). However, besides increasing security, all of these complicate the system and make it more difficult for employees to operate the computer.

(8) Another way to discourage potential hackers is through tougher legislation. Currently, laws regarding computer crime are not well defined enough to suit the many different types of crimes committed. But newer, more defined laws are slowly making their way to the Senate. For example, Section 502 of the California Penal Code defines a computer crime as "gaining access to any of these [computer devices] to commit fraud or extortion, gain money or services, or generally vandalize" (Wyden 70). Congress is now debating two computer-crime bills. The Computer Security Act of 1983 would create a fine of up to fifty thousand dollars or a five-year jail sentence for "robbing or abusing federal or private computers used in interstate commerce" (Marback et al. 46). The second bill, if passed, would set up an eighteen-month task force to look into the extent of computer crimes committed (Marback et al. 46).

(9) FBI task forces have cracked down on hacking rings and seized all their software and hardware in an attempt to defuse the situation. One well-documented case is that of the Milwaukee "414's" (so-named for the local area code), a group of teenagers who, before being caught, had broken in to more than sixty computer systems, including computers at New York's

Sloan-Kettering Cancer Center, Security Pacific National Bank, and the Los Alamos National Laboratory. Although little damage was done and nothing was taken, the potential to do great damage was in the hands of teenagers, again showing the need to regulate users' activities (Marback et al. 42). Another way the FBI has cracked down on hacker activity is by forming "tiger teams" of FBI personnel trained to recognize computer crimes (Alpern and Lord 48). However, it is still difficult to catch such criminals because "we're shooting at a moving target," says Daniel J. Cavanagh, vice-president of electronic installations at Metropolitan Life Insurance ("Computer Security" 126).

(10) Despite government attention, a re-enactment of War Games remains possible, although unlikely. Some government computers still remain connected to ARPANET (Advanced Research Projects Agency Network), a network set up for government use only, but highly accessible through local phone lines ("Pranksters" 54). The government has slowly begun to beef up its security measures and create a new computer network which will only be accessible from certain locations, thus eliminating the possibility for entry from unauthorized locations. But, as always, the high costs of security will be passed on to the taxpayers (Alpern 48).

(11) Instead of passing all these costs on to the average citizen, who has no intention of breaking in to other systems, why not regulate the potential hacker? The modem is the hacker's most essential tool, so why not require the modem owner to register his modem with the government? I suggest that modem manufacturers put a code, such as the modem's serial number, in the modem's permanent memory. Then whenever the owner uses his modem to enter a system, the receiving system will automatically be given this code. In this way, if the user does anything illegal, he will have left his "fingerprint" on the system. The government can then check this print against its file of modem owners and prosecute the guilty party.

(12) Ham-radio operators are required to register their radios. Modems are just another form of communication, so why not regulate them? This would eliminate the need for expensive security equipment. Eventually it would eliminate hackers and give us all a sense of privacy and security, knowing that "little Johnny" and his Atari 400 aren't destroying our checking accounts just for kicks.

List of Sources

Alpern, David M. and Mary Lord. "Preventing 'War Games.'" Newsweek 5 Sept. 1983: 48.

"Computer Security: What Can Be Done." Businessweek 26 Sept. 1983: 126-130.

Gillard, Collen, and Jim Smith. "Computer Crime: A Growing Threat." Byte Oct. 1983: 398-424.

Halper, Stanley. "How To Thwart Computer Criminals." Nation's Business Aug. 1983: 61-62.

Marback, William D., et al. "Beware: Hackers at Play." Newsweek 5 Sept. 1983: 42-48.

"Pranksters, Pirates and Pen Pals." Time 3 May 1982: 54.

Wyden, Ron. "Curbing the Keyboard Criminal." USA Today Jan. 1984: 68-70.