OCT 24 1983

Electronic Crime Wave

BEFORE high technology became an essential business tool, a manager could lock his cash and business secrets in the vault with reasonable assurance of their safety. Now computer systems have to be proved to be vulnerable to intruders in ways that previously were not possible.

In the first place, the victim business or institution may be unaware that its computer system has been invaded. If trouble is found, it may be difficult to determine whether the offender is a trusted employee, a mischievous teen-ager or a master criminal in another state.

Losses may be greater with computer technology than from crimes performed by older methods. Back in 1978, the FBI estimated that the average loss from an armed bank robbery was $10,000, while a computer crime expert estimated computer-related bank frauds and embezzlements resulted in losses averaging $430,000.

Stakes have gotten larger. A California man pleaded guilty to wire fraud by computer of $10 million from Security Pacific National Bank. While free on bail he hatched a scheme to steal $50 million from another bank and he is now in prison.

A Virginia man used his computer to get into files of Credit Bureau Inc. in Atlanta and used other people's credit cards to order $50,000 worth of merchandise by mail.

"The ripoffs are likely to be more frequent and larger," said a computer security specialist, observing that more people are learning about computers faster than precautions are developed.

His fears were substantiated a couple of months ago when a group of Wisconsin students were tripped up invading numerous public and private computer systems. Oklahoma students also have been found to be involved in similar activities, tapping into NASA and Defense Department systems, as well as GTE's Telemail system.

Proliferation of low-cost equipment makes it possible for almost anyone with the time and inclination to engage in electronic vandalism or big-time robbery. Authorities suspect that thousands of young people may be doing this sort of thing.

A Chicago student said those who got caught "really don't know what they're doing." What those who "know what they're doing" may be doing is anybody's guess.

Defense officials said computer meddlers did not obtain any really sensitive information, but a new movie portrays a teenager who altered his high school grades by computer and then set off a nuclear war via invasion of government computers.

That might be unlikely, but consider this possibility: The federal government maintains computer files on each individual an average of 15 times. Much of this income, health, pension and employment information is being passed from agency to agency. An interloper might obtain personal information that could be misused by tapping into any of scores of computer systems.

The many ways in which we might become victims of an "electronic crime wave" present an urgent need for protective laws and devices that are not yet in sight.