GEORGIA TECH RESEARCH

News Release
Research Communications Office
226 Hinman Research Building
Georgia Institute of Technology
Atlanta, Georgia 30332
(404) 894-3444

CONTACT: Mark Hodges/Ray Moore
(404) 894-3444

COMPUTER THEFT POSES
NEW PROBLEMS FOR SOCIETY

August 6, 1982

For Immediate Release

ATLANTA, Ga.--The computer revolution is forcing society to revise its definitions of theft.

Robbery no longer must involve a seizure of some commodity; it can be carried out as easily by punching the keys of a computer terminal to steal information.

"It's really impossible to define the level of computer theft going on in this country today, but my guess is there's a lot," says Dr. Richard DeMillo, professor of computer science at the Georgia Institute of Technology. "We see stories all the time in newspapers about someone who has broken a complex computer security system for the fun of it. There's just a flood of young computer programmers in America who bring the same enthusiasm to beating computer systems that they have for playing Pac Man. They want recognition. Unfortunately, there are also real thieves doing the same thing and they aren't announcing their achievements."

Robbery is as old as the human race, but DeMillo believes that computer theft poses new problems. In the past, when business was transacted with human hands, people were more careful about their dealings.

"Twenty years ago, you wouldn't have dreamed of not balancing your checkbook every month," DeMillo says. "But today many people have abdicated the responsibility for keeping tabs on their personal finances to the bank's computer. Our society has become too trusting in technology and not aware enough that it is subject to error or misuse."

DeMillo is troubled by society's unwillingness to consider computer information as property in the same sense as a house or machinery, even when a few electronic blips in a computer memory bank may represent data worth millions of dollars to a corporation. In his work as a consultant to industry, DeMillo has seen court cases where it became difficult to persuade a jury that a computer theft was as serious as a conventional robbery.

(more)

"People just have trouble accepting the fact that computer information has intrinsic value," he says. "Because they can't touch computerized data or feel it, they somehow can't accept it as property. That idea will have to be changed, as more of the world's financial transactions are carried out or stored in computer networks."

At Georgia Tech, DeMillo and his colleagues in the School of Information and Computer Sciences have carried out a number of research projects in the field of computer security. One result showed how insecure are computerized data banks maintained by the U.S. Census Bureau. (The Bureau wants to keep information on broad national and regional trends available to the public but without revealing information about individuals.)

Georgia Tech also has suggested methods for keeping computerized information secure in systems with multiple users, who are supposed to have varying degrees of access to the network's total information resources. (The military's complicated system of information classification is a good example of a need for a multiple use data bank.)

"I like to think of security as being similar to locking a bicycle in a rack," DeMillo says. "The size and expense of the lock are dictated by the value of the information. And though no computer 'lock' can be completely unbreakable, it can be large enough that any would-be thief would probably be noticed trying to crack it."

DeMillo has no easy answers for preventing computer theft. However, he suggests as a starting point that America do a better job of educating itself about the demands of a computerized business environment.

"We have to come to grips with the risks of using this kind of technology," he says. "That has to be pointed out to people. For example, when a bank issues an automatic cash withdrawal card to its customers, they shouldn't just be notified in fine print that they are responsible for losses from theft up to a certain dollar amount. That rule should be more prominently displayed. Every time we give up any decision making power to a computer, we should be told about it."

DeMillo also believes that high school classes which teach computer programming should give instruction in the ethical components of the business: that is, breaking computer systems isn't a game, it's robbery.

(more)

Finally, he stresses that the custodians of computer networks must not lull themselves into the delusion that their systems can't be broken and therefore need no physical protection.

"Everytime we come up with a new security scheme, a new weapon to break that system is going to be devised," DeMillo says. "Technology is never going to be perfect, so we should never forego physical safeguards for valuable information, like locks on terminals and guards at the door. If you remove humans from the security process, you're asking for trouble."