Thief proofing

MOHAN MURTI

You want to make your files secure, you say ? You want to lock up that vital information so that nobody can get at it ? You are shopping around for the very best in computer security systems so that nobody can steel your data ?

Forget it. There's a zillion programmes down at your friendly local neighbourhood pirate that promise to protect you. Not one of them is any more secure than your filing cabinet with a hefty lock.

Your lack of security from theft is a matter of law. Regulations are inspired by the United States of America, backed by American allies and enforced in many countries of the world.

The laws meant to protect the U.S. from foreign espionage have the unfortunate result of preventing the average user from locking up his computer data so that it is safe from prying eyes. The best you can do with any commercial security software programme is to make it very difficult for thieves and industrial spies.

Before you invest in any security system, you should know that if any other person or company really wants your secrets, there's nothing on the market that can prevent them.

It means, that software security systems ranging from little add-on utilies upto 10-disk monsters, ultimately all work the same way. The only difference among them is that the big ones provide successive barriers for hackers to break through and the little ones take just minutes to break.

Blame the U.S. National Security Agency (NSA) for all this. America's Super Secret Intelligence Agency, several years ago demanded and got laws that prevent marketing of any software package that can generate an unbreakable coding for information.

Such packages are, in fact, in existence today. But you can't buy them. They are for government use only, and if you ever manage to get hold of one, you are looking at a few years in the penitentiary, and so is the person who gave or sold it to you.

The reason is to prevent such systems from falling into the wrong hands of countries that are hostile or potentially hostile to the U.S. and its allies—like the Soviet Union. The U.S government's attitude on this and related matters of high technology is that if the Russians want high-tech, they can develop their own.

That seems fair enough.

The little known law came to light last year when the U.S. software company Persoft Inc. came out with its version 1.0 of a personal information manager called IZE. The programme included a password-and-encryption package for files it created.

Two weeks before IZE went on the market, Persoft received a visit from four polite gentlemen from the government. They explained the law to Persoft executives, patiently but insistently.

Persoft, it turned out, knew that they were supposed to file details of IZE's security package with the government before they marketed it. But they had forgotten this in the rush to put IZE on the market.

The upshot was that IZE was marketed without the security package, while they waited for government approval. This, in time, came, and IZE with the password-encryption device should be on the U.S. market by the time you read this.

Dual encryption now is common to most software packages. That is, any one who wanders into a protected programme or disk must first provide both a password (several passwords in sophisticated systems). Then, he must still prove details that will order the software to unscrable the coded material.

Passwords are virtually useless to a determined information thief.

That is because passwords must contain eight or fewer standard ASC II characters, basically meaning the 52 alphabet characters (upper and lower case) and 10 digits. That is a lot of possible passwords if you are writing them down, but because there are a finite number of passwords—around 200 trillion—a hacker can sift through the possibilities in a relatively short period.

The commercial encryption packages are generally even easier for the sophisticated thief who wants your marketing secrets. Almost all programmes merely convert readable ASC II-type files into binary codes.

These produce garbage on the screen when called up by casual thieves. But turning the garbage into usable information in child's play for any of the millions of computer experts in today's world.

In fact, there are computer programmes available on the commercial market that will sift password possibilities and decode binary coding into ordinary English (or any other language).

What you can buy down at the computer shop, then, will protect your vital information only as well as a safe and good locks protect the files you have on paper. The determined thief can get at it, given the time, and there is no such thing as "thief proofing."