Date Encryption using Truecrypt

Roger Bergstein
Stuart Computer Service
June 1, 2010

Today I want to talk about securing your data. Perhaps your business computer contains customer or patient records, credit card or social security numbers, etc. and your home computer contains banking and brokerage information. This information is also present on your backup device. If your computer or backup device is lost or stolen, this information is at risk. A technique I practice daily to secure my data is Data Encryption. Here is how it works:

I use a program called Truecrypt. It is a very small program consuming minimal resources, staying resident all the time. I instruct Truecrypt to create a password protected file of a predetermined size on my Hard Drive, which looks like any other file to the Windows. In fact, you can see the file using windows explorer. In reality, this file is my repository of secure data.

Back in the days of mainframes, we in the industry used the term *mount* when asking computer operators to make magnetic tapes available. Similarly today, Truecrypt's resident shell can, upon demand and entry of the password, mount the repository file and make it available to Windows as a virtual disk drive, for example, drive letter z. Word, Excel, Quicken, or any other program can read and write data to drive z, but the data passes through special encryption and decryption technology within the truecrypt resident shell. The data is physically stored in the repository file, but only readable and updateable when the repository file is mounted. Upon computer startup, with the repository file dismounted, the confidential data can't be accessed. The password must be entered when mounting the file.

When the repository file is dismounted, it can be backed up to a flash drive or external hard drive.

There is a special traveler version of truecrypt which will run on any computer without installation. So I can take my confidential data with me, and access it from any computer, after entering the password.