

Courant.com

How To Protect Computer Data

BOB JOHNSTON

September 19, 2007

With the state of Connecticut's latest debacle relating to the loss of notebook PCs from the state Department of Revenue Services, Gov. M. Jodi Rell has ordered that encryption be implemented on all portable devices. Encryption, however, is not an end-all solution.

Encryption is effectively the last bastion of defense against information compromise. That is, when all else fails, we hope that the encryption employed is adequate. Adequate? Yes, adequate! Encryption is simply a stall tactic. Given enough time, encrypted information can always be decrypted. The big question is whether the encryption is sufficiently resilient so by the time the key is discovered, the information protected is no longer valuable to the attacker.

With business plans, budgets, even battle plans, the value of information diminishes greatly over a brief period of time. But your personal information remains valuable for many years, perhaps 50 or more, and it is rare that encryption, which requires human interaction, is sufficiently durable. Simply stated, there is commercial software as well as free software that will attack encrypted data and ultimately succeed in deciphering the information.

Therefore, no one should breathe easier because the state plans to implement encryption on its portable computing devices. It needs to do much more. While it is desirable that faux pas by the state are promptly brought to the attention of the media and the public, this is not true when information is stolen, even if encrypted.

Most notebook computer thefts are a crime of opportunity. The objective of the thief is to turn the theft into cash. The black market desires to turn the device into a saleable product. To do this, they typically format the drive (erase the original information) and install a fresh operating system, after which it is made available for resale.

But if the thief is made aware through publicity that the information on the stolen device may be far more valuable than the physical object, it is entirely possible that an attempt will be made to sell it in the data market. Make no mistake, there is such a market and it is willing to pay far more for 100,000-plus identities than the local fence pays for the computer.

So what if it takes months to decrypt? Life simply goes on until the plaintext - the information in readable form - is revealed.

Within six months, more or less, the data market has more than 100,000 identities. Everyone

who has been notified that their personal information has been stolen is relaxing. Apparently, it has not fallen into the wrong hands. Then, those who take great pleasure in the art of plundering accounts of those who are susceptible begin their work.

Thankfully, the governor has specified that other controls should be implemented. Nevertheless, one must wonder why at least two additional controls that do not cost a single penny were never implemented. These controls are available on all notebooks manufactured today, and most going back to 2000 or even earlier. I have a notebook manufactured in 1998 that supports the controls, the first of which is built into your notebook. It is called DriveLock. Unlike the logon password or BIOS password, the hard drive password is stored only on the hard drive and remains even if you move that drive to another PC.

It is not impossible to circumvent a hard drive password, but is extremely difficult. Most of the information on the Internet in this regard is largely inaccurate. If you own a notebook you should have implemented the hard drive password. It is accomplished via the BIOS, although the BIOS does not store the password. A minor inconvenience each time you reboot, but well worth the satisfaction should your notebook be misplaced.

Now, how about a tool that causes your computer, notebook or desktop, to call home should it be stolen and provide the information needed for law enforcement officials to locate it and is also FREE? The tool is called LocatePC, and you can learn more about it at www.iconico.com/locatePC/. Be sure to follow the instructions to ensure that you receive the information that LocatePC will produce.

Now, why in the world didn't the stolen PCs, nearly 30 at last count, have these two tools implemented? I do not know but feel that you and I, the public, have been placed in unnecessary jeopardy.

Bob Johnston is chief security adviser to ASC, a computer security and services company in the Broad Brook section of East Windsor and has been responsible for the security of sensitive digital information worldwide for more than 35 years.

Copyright © 2007, [The Hartford Courant](#)