Laptop Thefts Increase

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Laptop computers are ideal for thieves. They’re small, it looks normal to carry them (in contrast to, say, file servers), they can be sold as used computers via electronic auctions and sales channels, and – best of all – they may information that can be valuable to the right people.

Estimates from the people who make laptop security devices claim that 15% of all laptops are stolen every year worldwide. Although this could be a high estimate, it’s still a real problem. Laptops get stolen from cars, in planes, and even at security checkpoints in airports. It bears repeating that the security-gate scam is particularly effective: one thief goes through before the victim and the second thief delays the computer owner by “finding” additional metal objects in surprising quantity every time (s)he goes through the metal detector. By the time the owner gets through, the computer is gone.

In a recent article entitled “Agencies Have Lost Hundreds of Laptops; Justice Department Says Computer Theft Is a Growing Problem” by Brad Smith of _The Tampa Tribune_, the writer highlights the growing severity of this problem. Some key points made by Mr Smith:

* According to Jerry Rubino, the director of security and emergency planning at the Justice Department, hundreds of government laptops have been stolen out of thousands in use.

* Two laptops were stolen from the MacDill Air Force Base in early August; there is unconfirmed speculation that they contained classified information.

* The Inspector General of the Department of Justice has reported that “five agencies, including the FBI and DEA, have lost track of 400 laptop computers, more than half of which may have contained sensitive national security data.”

* “The IRS has lost or misplaced 2,322 laptop computers, desktop computers and computer servers over the past three years.”

* Foreign governments also report laptop thefts: 600 from the UK Ministry of Defense since 1997; 500 in Australia in a single year, some with sensitive government information.

Depending on your circumstances, the loss of a computer may be a minor inconvenience; you can even buy insurance to recover part of the cost. And with computer prices dropping, the depreciated cost of an older laptop may easily cover the cost of a new replacement. However, the loss of control over confidential data may be a disaster. Think about the kinds of information that you or your executive users are carrying on corporate laptops; for most of us, the thought of having strangers ferreting through customer files, employee records, strategic plans and internal e-mail messages sends a chill up our spines.

To reduce the damage from lost and stolen computers, all of us should be encrypting sensitive data on our laptop computers. I use the PGPDisk function to sequester all sensitive information, including client files and student records, on my laptop. The encrypted partition looks like a disk
to the operating system and is painless to use: I just have to enter a passphrase to mount the disk when I boot up the computer. However, any thief who tries to read my data without the passphrase will find them completely uninterpretable. It won’t even be possible to see the directory and filenames.

Similar protection is available with various operating systems that include encrypting file systems.

The cost is negligible; just do it. Today. Now.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.