Maryland Entrepreneur Quarterly

Reprinted with permission from The Business Monthly, Inc.
September 2010

Is Your Laptop Secure?

By Heinan Landa

It's a question that should make you stop and think. In fact, you may be in a coffee shop right now reading this article and saying to yourself, "Of course my laptop is safe; I'm always with it."

Except when you're not, like 10 minutes from now, when you have to go to the restroom. Or the next time you are travelling for business and leave your carry-on items (including your laptop) under the supervision of your new "friend" who is engrossed in his *Wall Street Journal* while you run to the restroom.

In fact, according to Safeware, a company that specializes in insuring high tech equipment, a laptop is lost in an airport every 50 seconds. Don't become part of that statistic. Learn the top five steps you can take to secure your laptop and roving data.

1 Back up your laptop files. Your organization probably has an effective backup plan in place for your network. But did you account for your laptops? What is the backup plan in place for those files? What about your personal laptop? Unlike your desktop PC, your laptop is usually not plugged into the network on a regular basis; it is turned off at night when organizational backups are done. Here are your options.

- *Internet-based backup system (the easiest option):* With Internet-based backup systems like mozy.com and carbonite.com, you can set up your account to back up your laptop every time it connects to the Internet. The drawback? Your files are only backed up and stored for 30 days.
- *Network-based backup system (the technically trickiest option):* With this method, you configure your laptop so that whenever you connect to the network, it synchronizes your files back onto your company's server. The drawbacks? This method is time intensive for the user, and not everyone connects to the network frequently enough to make it worthwhile.
- *Automatic backup system (the option of circumvention):* If you are using your laptop only to take control of your desktop remotely, you are in the best position possible. Once you log in, all of your work is actually being done on the network; there is no need for an additional backup method. The drawback? This isn't a real possibility for most laptop users because it requires continual, fast Internet access.

2 Password protect your entire laptop. Think you've already got this one covered because you have a basic Windows login password? Think again. Your windows login password will only help to discourage the novice laptop crook. The more advanced thief will find a way to get to your data.

That's why you should configure a hardware-based system password that you are required to enter each time you start your computer. This will prohibit any access to the computer at all.

3 Consider a LoJack for your laptop. The same GPS-like software you can put on your car is also available for computers. You can order the LoJack software and install it on your machine. If someone steals your computer, as soon as that person uses it to access the Internet, the LoJack software sends notification to the monitoring center. This center grabs the IP address that the stolen computer is using to log in and can then track your laptop's location.

4 Encrypt your hard drive. This is essential, especially if your laptop contains sensitive data. A password won't stop hackers. Once they have your laptop, they can take your hard drive and put it in a different machine as a secondary hard drive and access your data without your password.

Purchase software that will keep the contents of your hard drive in a strongly encrypted format and provide you with transparent access to the data from any application. The software will scramble your data as you save it to your hard drive and will require a password at login to access the key to un-scramble it. Many newer laptops come with encryption as a built-in feature.

5 Institute and enforce a laptop policy for your organization. If you manage an organization, you probably have policies for just about everything — except laptops. Change that today. Create a policy that requires all employees to accept financial responsibility for their company-issued laptops if they should lose them. With a policy in place, employees are more likely to keep laptop security top-of-mind. Hold employees accountable by requiring certain security measures like the ones mentioned above be implemented when their laptops are in use.

Laptop security is more complicated than it sounds. A multi-faceted approach to mobile security and data protection is necessary. To decide which security methods should be implemented, evaluate the sensitivity of your organization's data, your laptop usage and the culture of your company. Then, create a policy — and enforce it.

Heinan Landa is the president and founder of Gaithersburg-based Optimal Networks (www.optimalnetworks.com), a comprehensive computer and network support services firm assisting small to mid-sized businesses. Contact him at info@optimalnetworks.com.