

---

# Keeping It Safe and Protected: The Mobile User (Part II)

By Craig D. Collingwood

**Editorial Abstract:** Mr. Collingwood looks at a combination of behaviors and technologies to help laptop computer users safeguard sensitive data. He discusses recent threats, modern data protection methods, and best practices for travellers and Internet cafe patrons.

Part I of this article appeared in the Winter 2006 edition of *IO Sphere*.

In our first installment, we focused on the physical security of the laptop, personal digital assistant (PDA), or cell phone, and how to prevent the loss of the equipment. This article will focus on protecting the data contained within the physical device if it is taken, lost, or compromised through inadvertent disclosure while unattended, or while working in a crowded area.

To give an example of the lengths people can go to get information from a laptop, I will use an actual incident that happened to a team of travelling investment brokers. The travellers took a laptop on a business trip to Europe. When going to dinner, they left the laptop in their hotel in what they thought was a secure location. They were gone from the room for a couple of hours for dinner. During that time someone entered the room, disassembled the computer, removed and cloned the hard drive, and then reassembled the laptop. Several months went by before the company discovered the event. They later estimated that data's value to be around seven million dollars. While this is an extreme example, is not so far out when you consider the range of potential values of the data on your laptop.

Personal data, corporate sensitive data, classified data, and the cost of laptops makes them prime targets for thieves and the number stolen each year continues to grow. Just this past summer here in San Antonio, Texas, the new Toyota manufacturing plant reported the theft of one of their laptops which contained a list of all employees and their social security numbers. This opens up all of those employees to potential identity theft, and years of trying to rebuild their credit after being victimized.

The first rule of thumb is to be aware of the area that you are working in, and the sensitivity of the data you are working on. Targeting any device for the value of its data is much easier in a crowded airport, restaurant, or coffee shop. So-called "shoulder surfing" from a strategically placed chair or table enables others to see the data you are working on, to evaluate its potential corporate sensitivity, and possible piracy value to your competitors. Suppose you're working on your laptop and the person next to you seems to be glancing toward, or



*Is your data secure? (Datavault Corp.)*

actually reading your work. Is it innocent curiosity, boredom, or someone looking to see if your laptop is a good candidate for data theft?

To protect your data you can do many different things:

- Use a firewall software program to protect your system from outside intruders when on the internet.
- Turn off printer and file sharing.
- Keep your virus signature files up to date.
- When connecting to other networks use virtual private network (VPN) software to connect back to the company or a customer site when traversing the Internet. This will encrypt the data as it is being transferred from your laptop to the network, and back again.
- Keep the data separate from the system by copying it to an external storage device like a thumb-drive, CD-RW, or a writable DVD. Make sure that you use this as the default storage location for all of your data files and personal information, so if you lose the laptop you will still have the data.
- Encrypt all important files.
- Purchase or invest in security configuration testing software to help you evaluate the security level of your computer before you travel.
- Make sure when traveling to try and find hotels that enforce password and login requirements on their wireless Internet services, to prevent or at least deter network interlopers. Such intruders may peruse unsuspecting users' hard drives looking for valuable data—or worse, walk into your corporate network through the "door" you have provided.



*Too much laptop sharing? (US Government)*

- Keep all personal information and private accounts such as: credit card and bank accounts, social security numbers, home address, personal information, and other passwords off of all systems that will be directly connected to the Internet.

- Use complex login passwords consisting of special characters, upper and lower case letters, numbers, and which do not have dictionary words as part of the password. A phrase is easier to remember and will help keep you from having to write it down. “Tell Me What To Do For You” could equate to a password of Tmwtfdy%1 when you add special characters and numbers into the mix. The password should be a least 8 characters long; the longer the password, the harder it is to decrypt or guess.

Newer computers come with many different means to help you protect your laptop, both during use and when you choose to turn in or dispose of your current laptop. Some come with multi-login methods to help increase data security, such as thumbprint readers or smartcard readers. Bio-metric login hardware is now an option you can add to your laptop to help increase the security and protection of your data. Several vendors are advertising a thumbprint reader on new laptop product lines.

Some laptops and operating systems are coming out with encryption and decryption software, providing further built-in security for your really important files. Additionally, there are new programs designed to completely erase the laptop’s hard drive and memory before you turn it over to another individual.

At least one major manufacturer is working on a new chip which locks the hard drive, so that when removed from the laptop, it becomes totally useless. The embedded chip will provide increased data, e-mail, and credential protection via enhanced encryption. Another option on some laptops is a software package which locks out Universal Serial Bus (USB) and removable media except to authorized administrators and power users. It also limits write access to optical drives, and limits access to serial and parallel ports, making it harder to access and duplicate the without your knowledge or approval. Keeping abreast of these and similar innovations further increases computer and data security

Some computer manufacturing companies are even providing a laptop tracing hardware tool that will allow you to track your laptop and determine its exact location in the event that it is taken. Once reconnected to the Internet, the stolen laptop e-mails its exact location to a predetermined e-mail address. This provides police or other law enforcement agencies a good chance to apprehend the individual with the evidence in hand. Low-level formatting of the hard drive does not remove this application, so adding it to your security package could be a good investment. Current per system costs for this type of locator package is approximately US \$149 - \$200. However, the money you could lose in both hardware costs and data values might easily make it worth the investment.

The US Congress continues to pass new laws as the threat of data piracy becomes more prevalent, and increasingly more complex. Corporations have been pushing hard for legislation to stiffen the penalties, and increase sentences for data piracy and hacking. Ideally, more laws and stiffer enforcement should result in an increase of the number of people tried and imprisoned for violating those laws. But a serious threat remains, and a multi-layered approach is still the best defense.

The future of data protection looks bright, but will always require each and every individual to keep a vigilant watch. We must be constantly looking for those who want to illegally profit from data piracy, and gain corporate and governmental data by any possible means. But no matter how many new technologies, laws, or innovations we develop to protect our data, it will be up to each of us. Stay sharp, and remain alert. Every day we are entrusted with the hard work of others, and we simply must protect that trust. No matter what protections are built into the system, if you do not practice good data security, they become useless. Always remember: security begins and ends with you. ☹

Craig Collingwood is a consultant with Hewlett Packard’s Federal Technologies Solution Group. Mr. Collingwood served in the US Air Force as a Computer Systems Programmer. He has over 29 years corporate experience in information UNIX system management, programming, computer security, and systems configuration for organizations and companies such as the US Air Force, Digital, Compaq, and Hewlett Packard. Mr. Collingwood currently provides network support for the JIOC/J6.