

Keeping it Safe and Protected: The Mobile User

By Craig Collingwood J63

Editorial Abstract: Mr. Collingwood outlines a common sense approach to protecting sensitive, highly portable data devices.

With the ever increasing numbers of mobile users come new problems and concerns about keeping the corporation data and networks protected and secure. As more and more travelers are carrying laptops, Personal Digital Assistants (PDA), smart phones, and other computer devices the issues of physical security, data security, and network connectivity are becoming an increasing burden on everyone.

With portability comes the increased risk of data compromise due to hardware loss or theft, increased security risk, and the prevention of infected computers coming back from the field and connecting to the internal networks. The mobile traveler must become an integral part of network and data security, to help protect not only their physical devices, but the networks they connect to when they arrive back home.

According to many studies corporate data theft is on the rise and one of the easiest targets can be the mobile user and the equipment they take with them while on the road.

With corporations becoming more concerned about data and networks security on their internal networks it is becoming easier to gain information by stealing data or equipment from traveling representatives, rather than hacking into the corporation's internal networks. Non-secured computer equipment is a target for both corporate saboteurs, and the common thief who is looking to make a quick buck.

In the last year there have been several incidents of corporation data being obtained and possibly misused by the loss of a mobile device when traveling. March 28, 2005 an individual walked into the University of California, Berkeley office and took a laptop system. The computer contained over 100,000 alumni, students, and graduate applications containing SSN, addresses, telephone numbers, birthdates, and income information. April 2005 a laptop was taken from a MCI managers car while parked in his garage at home. The laptop contained 16,500 names and SSN's of MCI current and former employees. May 2005 a laptop was stolen from the Omega World Travel of Fairfax it was believed to contain travel account information for 80,000 Department of Justice

employees. These thefts all have long term ramifications for the people whose data is on those laptops.

As we continue to make the equipment smaller and lighter they have become easier and easier to misplace. Have you left your cell phone, PDA, or other devices in the car or taxi when you go to a restaurant or into the hotel for the night? Have you every left those same devices in the hotel room as you go out for the evening thinking the items are secure behind a locked door? This leaves the device open to theft either for the value of the use of the item, the possible data contained within, or its potential resell values to those with less than honorable intentions. Of course, there is the potential for the international long distant call charges that go with the loss of your cell phone. "The loss of a handheld device containing sensitive information is a very real threat. A recent survey by Pointsec Mobile Technologies shows that, over a six month period, 21,460 PDA/ Pocket PCs and 85,619 mobile phones were left in the back of cabs in Chicago alone." (Portable Devices)

Securing a laptop using a cable lock and alarm system has been preached for years. Have you taken the time to pull it out and secure your laptop before you leave the hotel room at night? I would wager that most of us have not, and wouldn't know how to do it if we chose to start doing so. Ensuring the physical security of these high theft items is a key element for the mobile traveler to protect the systems and the data they contain. It is time to step up to the plate and become more pro-active in protecting these mobile systems, despite the hassles and time involved in doing so.

The next time you travel try to keep your system safe, protected and close by - to keep the bad guys from taking it out and selling it to the highest bidder - either for the data it contains or the monetary value of the device itself. Next article will concentrate more on the security of the data on the mobile devices and some steps that can be taken to help protect the data from prying eyes, or corporate spies. Remember to keep it safe and protected when you are out there.

References:

Olzak, T., (2005). *Portable Devices*. Retrieved August 31, 2005 from the SecurityDocs.com web site: http://www.securitydocs.com/Wireless_Security/Portable_Devices

