

MEDIA STATEMENT

PROTECTION NEEDED TO PREVENT DATA THEFT FROM LAPTOPS

Friday June 6, 2003

A West Australian company says it can help prevent data being accessed from thousands of laptops being stolen from Australians every year.

Many stolen laptops are loaded with sensitive company information, and possibly even offer access back into company networks and employee information.

Secure Systems Limited Chief Executive Officer Mike Wynne said his Perth-developed Silicon Data Vault, (SDV®) is a unique hardware-based security device, which uses early boot authentication for access control and encryption for data protection. .

Mr Wynne said the SDV® was the first system in the world to combine hardware, encryption, pre-boot authentication and controlled partition access.

“The SDV® is incorporated with the Hard Disk Drive (HDD), intercepts the boot process, and forces the user to authenticate to the device before confidential files or data can be accessed,” he said.

According to the Australian 2003 Computer Crime Survey laptop theft has almost doubled since 2002. The quantifiable loss from 82 respondents was over \$2.2 million.

“Financial loss due to laptop theft is now the number one type of loss, last year it ran second behind virus infection,” Mr Wynne said.

“While laptops are great for mobility, surprisingly they are most often lost or stolen from corporate premises - not from users while traveling.

“But what is alarming is that informal surveys indicate more than 15 percent of laptops are stolen by criminals intent on selling the data.”

A recent study conducted by the FBI found that 57% of computer crimes were linked to stolen computers that were then used to break into computer servers. (deleted later on)

Only last month 13 laptops containing confidential information on murder cases, sex crimes, armed robberies and drug charges were stolen from Melbourne’s Department of Public Prosecutions. The laptops were valued between \$45,000 and \$60,000.

Mr Wynne said laptop computers were an ideal target for thieves.

“They’re small and it looks normal to carry them, they can be sold as used computers via online auctions and sales channels, and - best of all - they frequently contain information that can be valuable to the wrong people,” he said.

“To reduce the damage caused by lost and stolen computers, all of us should be encrypting data on our laptops – using a system such as the unique (SDV®) which provides automatic encryption and is transparent to the end user.

“Companies are discovering that a traveler's stolen laptop is more than an inconvenience — it's a dangerous security risk.”

Tips for keeping laptops safe:

- Carry your laptop in an unidentifiable case, like an over the shoulder canvas bag.
- Be careful when going through airport security check points.
- Change your password regularly for access to your laptop.
- Lock away your laptop in your office or hotel room while not in use.
- Protect your data by using hardware encryption.

MEDIA CONTACT: Donna Cole – 0419 901 229m or lastsay@bigpond.net.au