Laptop Security

By Mark Sayer, Principal Security Consultant

Laptop Use

While many regard the 1990's as the decade of the Internet, there is no doubt that we are currently in the age of mobile everything. From laptop computers to mobile phones, wireless and mobile communication is increasingly prevalent. The surge of mobile-computing innovation has brought enormous benefits to business and consumers alike, but it has also left many security professionals facing some alarming security challenges.

One of the most significant trends in corporate information technology over the last five years has been the increased usage of laptop computers. Once only the domain of executive management and for special mobile applications, laptop computers are now routinely issued to middle management and IT personnel, and some organisations have completely replaced desktop computers with laptop computers.

A number of factors have contributed to this trend; some of which are:

- dramatic falls in the cost of laptop computers (2005 saw the first sub $1,000.00 laptop computer hit the Australian market)
- exemption of laptop computers from fringe benefits tax (allowing many employees to salary-sacrifice the purchase of a laptop)
- the perception of laptop computers as a 'status symbol'
- more flexible working arrangements allowing employees to 'telecommute'.

Laptop Theft

The increased abundance of laptop computers in the workplace and the home has resulted in a proportionate increase in the number of thefts. Laptop computers have now replaced cash as the prime target of burglars and opportunistic thieves, according to Tony Jackson, principal of St. George Underwriting Agency who insures many of Australia's corporate laptop computers. Jackson says the company's claim records shows that one in every 20 to 25 notebooks are stolen, broken or destroyed.

According to NSW Bureau of Crime Statistics estimates, 3.4 per cent of laptop computers are stolen each year, with similar figures reported in Victoria. Australia-wide, this represents a loss in excess of $30 million. The 2005 CSI/FBI Computer Crime and Security Survey found that the theft of laptop computers ranked as the second most common security incident experienced by organisations this year. Gilles Novel, managing director of Business Security Systems Australia, says the reported figures are not necessarily a true indicator of the actual incidence of theft "because people without insurance wouldn't bother making a report".

The AusCERT Australian Computer Crime Survey found that the average reported cost of replacing a stolen laptop was in excess of $17,000.00, when taking into account the cost of replacement hardware, IT resources to re-install and update operating systems and applications, recovering lost data and employee down time.

However, none of these statistics take into consideration the potential loss of confidentiality of information stored on stolen laptop computers. In our efforts to calculate projected return on investment figures for clients considering our security awareness training program, we were alarmed at the number of organisations we spoke with who said their CEO's laptop was stolen within the last year. In fact, it seems to be a common belief that CEO's are amongst the least security savvy people and that's why they are always losing their laptop computers. However, when six or seven companies in a row all cite recent incidents of their CEO having a laptop computer stolen right off their desk, you do begin to wonder.

Just ask Irwin Jacobs, CEO of Qualcomm, who had his laptop stolen from the podium at a presentation in September 2000. In front of a number of witnesses, Jacobs stated that the laptop contained highly sensitive information that would be of great value to foreign governments. At the time of this incident, Qualcomm was in negotiations with several of China's telecommunications providers to license their CDMA technology.

continued page 2

continued from page 1

Preventing Laptop Theft

When looking at the particular circumstances of laptop thefts, it becomes immediately apparent that the vast majority of these losses can be easily prevented. Aside from specifically targeted thefts, most thefts are opportunistic. Typically, someone will walk in from the street, pick up one or two laptops left unattended on desks and then simply walk out with them. There is also a growing trend of thieves walking around shopping centre car parks after working hours looking for laptop computers left in cars while employees 'duck-in' for some last-minute dinner ingredients on the way home from work.

A targeted program of raising employee awareness about the risk of laptop theft is without a doubt the most effective means of preventing loss. As an example, if people are aware that there is a very good chance their own car window will be broken if they leave their laptop inside the car, they will be much less likely to do so. In addition to raising awareness, there are a plethora of controls available to deter, prevent and aid in the recovery of stolen laptop computers. Following is an overview of some of the most common controls available today.

Deterrents

Warning stickers
Simple stickers warning that laptop computers contain hardware security controls rendering the machine unusable without the password or threats that the computer is tracked electronically, provide an excellent deterrent, especially from the less computer literate thief. Also, engraving the laptop computer with the organisation's details offers a good deterrent as it can significantly reduce the street value of the stolen laptop.

Companies like Computer Security Products in the U.S. provide excellent stickers that not only act as a deterrent but can also assist in the recovery of stolen equipment by leaving an etched message upon removal of the sticker.

Appearance of security
Other physical security controls within the environment, such as well maintained fences and access controlled doors, security badges, warning signs and on-site security guards can help deter would-be thieves from entering the premises in the first place.

Encrypted hardware
Several leading laptop manufacturers now include models with built-in hardware encryption that will render the hard disk in the machine useless without the password. Since the cost of replacement of these hard disks can be more than the street value of the machine, it becomes unprofitable for the thief.

Prevention

Awareness
Provide employees who are given laptop computers with some training on the security and safety risks associated with laptops before or at the time they take possession. Place awareness notices in company newsletters, including details of any recent cases of laptop theft experienced by the organisation. Emphasise the benefits to them personally from protecting their laptop computer hardware and information.

Cables and locks
Laptop cables and locks, including the Kensington lock, are the standard means of physically securing laptop computers. While these are effective at preventing quick thefts, they are ineffective at preventing thefts where the thieves have a reasonable amount of time and/or are in a position where they can operate without detection (e.g. in an office during the weekend or in an unattended meeting room).

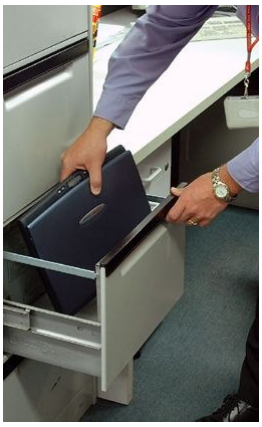
Proximity detection
This popular device is very effective at helping to prevent laptop theft while travelling. A wireless device within the computer polls a device held by the custodian of the computer. When the two are separated, a loud audible alarm rings, making it easier to track the thief with the laptop in a busy train station or airport, for example.

continued page 3

continued from page 2

Out of sight

Make sure that employees don't leave laptops lying around after hours. Security personnel or their delegates should always keep an eye out for unsecured valuables in and around the work environment, especially after normal business hours. If unsecured business or personal assets are noticed, the relevant staff member should firstly be reminded of the need to protect property.



Repeat offenders should be disciplined, either through loss of privileges, or other action as sanctioned in the organisation's security policy.

Recovery

Software tracking

Several companies provide computer software solutions that make the laptop computers contact a central monitoring system when they are connected to the Internet. Most of these systems will continue to work even if the hard disk is formatted and re-installed with a new operating system. Some of these companies even provide financial guarantees that they will be able to recover any stolen laptops with their system installed within a defined timeframe.

References

Knowledge on the move
http://www.theage.com.au/articles/2003/11/10/1068329474897.html?oneclick=true

Labmice laptop security guidelines
http://labmice.techtarget.com/articles/laptopsecurity.htm

S.T.O.P. theft prevention
http://www.computersecurity.com/stop/prevention.htm

Kensington locks
http://www.kensington.com/html/1434.html

Computrace laptop tracking software
http://www.absolute.com/

Stealth Signal XTool laptop tracking software
http://www.stealthsignal.com/

Scambusters, one of my favourite sites
http://www.scambusters.org/laptop.html

A good article on laptop security
Part 1 - http://www.securityfocus.com/infocus/1186
Part 2 – http://www.securityfocus.com/infocus/1187

2005 AusCERT Computer Crime Survey
http://www.auscert.org.au/render.html?it=4579

2005 CSI/FBI Computer Crime and Security Survey
http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

neocomm

About us

NeoComm is an established Australian protective security consultancy firm with a solid reputation for delivering quality services that are exceptional value for money.

Just some of the many services NeoComm provides are:

- → Penetration Testing
- → Physical and Information Security Review
- → Security Awareness Strategies and Training
- → Vulnerability Assessment
- → Risk Assessment
- → Security Policy Development
- → Web Application Security Architecture

Contact us

t: 61 3 9894 7720

Suite 155, 199 Toorak Road
South Yarra Vic 3141

e: info@neocomm.com.au

Visit our website www.neocomm.com.au