

Laptop Security



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 is 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 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. 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

Security News bits



Secure Media & Promotions merges with Amlec House

Amlec House Pty. Ltd., a security and risk management consultancy has merged with Secure Media & Promotions, a provider of security e-learning and awareness packages.

<http://www.neocomm.com.au/news/>

NeoComm signs agreement with Amlec House

NeoComm signs agreement with Amlec House to distribute Security Awareness Training to West Australian organisations.

<http://neocomm.com.au/news/>

Phishing attacks on the increase

By the end of 2004, Symantec reported an average of 33 million Phishing attempts per week. This shows just how popular these online scams are becoming.

<http://itvibe.com/news/3377/>

Dates of interest



Global Security Week

The week leading up to September 11th is Global Security Week.

<http://www.globalsecurityweek.com/>

Ruxcon

1st - 2nd October 2005, Sydney

RUXCON is a conference organised by and for the Australian computer security community.

<http://www.ruxcon.org.au/>



Visit www.neocomm.com.au to find out how easy it really is to establish a security culture with NeoComm's Security Awareness iLearning solution.

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.

To learn more about how to prevent laptop theft, read the full article at <http://www.neo-comm.com.au/articles/>

Useful Links

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

<http://labmice.techtarget.com/articles/laptopsecurity.htm>
Labmice Laptop Security Guidelines

<http://www.computersecurity.com/stop/prevention.htm>
S.T.O.P. Theft Prevention

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

<http://www.absolute.com/computrace>
laptop tracking software

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

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

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

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

Staff Profile



Mark Jarratt CPP, Senior Security Consultant.

Mark specialises in analysis of the corporate protective security profile, physical security assessments, policy developments, security audits and Commonwealth protective security compliance.

How long have you been in the security industry?

I was a Customs Officer from 1980 to 2001 and was involved in border security issues for much of that period, including as an enforcement, search and patrol officer on the Sydney waterfront and at Kingsford-Smith international airport. In 1994 I was appointed chief of security and agency security adviser, national office, Australian Customs Service, Canberra. I held that position for almost 5 years and became a private sector protective security specialist in August 2001.

Tell me something interesting about your background before NeoComm?

Founding member (drummer) of original 'guff rock punk band "The Chancres", and writer of about 20 songs. Now quite deaf. Over 20 years as a musician with widely varying success, playing both kinds of music (Country AND Western).

Lived in Britain and Israel/Southern Lebanon. Worked as a business analyst for the Hong Kong Customs & Excise service and was a member of an expert APEC team delivering customs technical training in USA, Taiwan, China, Vietnam and Chile.

What is one of the best achievements you've accomplished in your job?

Appointed as Chairman of Australian Chapter, ASIS International.

Winner of Australian Teachers of Media first prize for best instructional and training video, and ASIS International Silver Award, Audio-visual category (government) - 'Mission Improbable' privacy and security awareness kit, Customs. ASIS International Certified Protection Professional - Board Certified in Security Management.



What do you do when you're not working?

Sleep, read, eat, and play with my 6yr old son Kyle. Travel to Sydney to be with my spouse Dr Angela. Avoid housework.

What are your interests?

Advancing the professionalism of security practitioners through my voluntary role as Chairman, Australia Chapter, ASIS International. Lobbying for justice for high income non resident fathers in the Child Support system.

Case Study



Orica, one of Australia's largest public companies, is a group of four business platforms – Orica Mining Services, Fertilizers (Incitec Pivot Limited), Orica Chemicals and Orica Consumer Products – who are all market leaders in their respective industries and enjoy world class reputations.

Orica's Information Security Manager, Mr. Michael Jerkovic, is responsible for the company's information and technology security.

When Mr. Jerkovic first looked into NeoComm's Security Awareness Training program, his primary concern was, *"the Orica security policies and procedures were not being effectively communicated to staff. Security incidents occurred would have been prevented had the staff been more aware. For example virus incidents were tracked to staff opening email attachments from people whom they did not know. Laptops were also being stolen by unauthorised people who were allowed to enter the office unchallenged"*.

While Orica had provided some staff with face-to-face security awareness training in the past, they found that this method proved to be somewhat difficult. According to Mr. Jerkovic, *"it limited the number of people who were able to participate"*. This is because traditional face-to-face delivery methods take staff away from their day-to-day duties, and in Orica's particular circumstances, made it almost impossible to run security awareness training in remote areas where only a

handful of employees were situated.

Mr. Jerkovic also found that NeoComm's Security Awareness Training program *"covered a scope broader than just IT security, it also included physical security, security outside the office and security whilst travelling, which is important to us as a global organisation"*.

When asked what features of NeoComm's Security Awareness Training were most important to Orica, Mr. Jerkovic said, *"the best feature of NeoComm's training is that it is delivered in an entertaining fashion. Security awareness is a fairly dry topic and NeoComm has found a way to introduce it in a format which will not send you to sleep. This is important since you want your staff to comprehend the material"..."Bookmarking is an essential feature that allows staff to complete the training over a number of sessions."..."My requirement to track and record the progress of the users as they complete the training is ably met by NeoComm's training"*.

The smooth implementation of NeoComm's training provided minimal interruption to the business. Since the training was launched, the vast majority of staff who have completed the program have given very positive feedback.

Whilst the training has been very effective, Mr. Jerkovic believes that the overall security culture of the organisation may take some time to change, and that *"NeoComm's training has provided the ideal start to this change"*. According to Mr. Jerkovic, *"every organisation should provide security awareness training, and Orica is very satisfied with its choice of the NeoComm solution"*.

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 & Information Security Review
- Security Awareness Strategies & Training
- Vulnerability Assessment
- Risk Assessment
- Security Policy Development
- Web Application Security Architecture.

We can tailor a service to your needs, contact us today.

Contact us

t: 61 3 9894 7720

e: info@neocomm.com.au

Visit our website <http://www.neocomm.com.au>

If you know of anyone who might like to receive our newsletter, please forward their email to us. Naturally, we will keep theirs and your information strictly confidential.

To unsubscribe [click here](#).

Or send an email to info@neocomm.com.au with unsubscribe in the subject.