



THE Daily Telegraph

Size: 94.03 sq. cm.

Date: Wednesday, 30 November 2005
Page Number: 6
Edition: First
Supplement: Connect

Market: NSW
Circulation: 397,915
Published: MON TO SAT
Editorial: [email the editor](#)
Item No: P8479268



cutting edge

> secure business

The latest research conducted by IT solutions company Altiris has uncovered some alarming results for Australian businesses.

According to the SpectroTech 2005 IT Security Vulnerability Report, a large number of organisations are leaving their corporate networks open to attacks by hackers.

The report, researched across Sydney, Brisbane, Melbourne, Perth, Adelaide, Hobart and Canberra, says weak WLAN (wireless local area network) security would be the target for network intrusions. Results showed 18 percent of CBD-based companies were using default configuration settings for their wi-fi access points. Default settings, including names and passwords, are easy for hackers to compromise and gain access to a network.

And an alarming 27 per cent of businesses made no attempt to secure their wireless networks with encryption keys.

“Adelaide’s CBD-based companies are the biggest offenders at 36 per cent,” says independent IT security expert Laura Chappell.

“This figure is extremely high. If confidential information is crossing the wireless network in plain text, then that’s handing corporate secrets to the competition on a platter.”

Some 70 per cent of businesses within Australia’s CBDs use WEP (wireless equivalent privacy) as a security shield for their wireless networks.