



## TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial  
arrangements with vendors.

For more reviews, please  
contact TECHNOLEDGE.

T +61 2 9909 0246  
E [info@technoledge.com.au](mailto:info@technoledge.com.au)  
W [www.technoledge.com.au](http://www.technoledge.com.au)

## The Security Landscape

### A Guided Tour

#### PART 1 – TREACHEROUS TERRAIN

Computer Security is a business full of spies and counterspies who communicate in secret code. Like Interpol, antivirus vendors have had a hard time keeping up with the crooks. The Stration worm caught some of them out last year - antivirus engines have little trouble detecting the virus or worm in a 'blended threat' but sometimes don't see the payload it carries until it's activated.

Security vendors claim their products protect us from harm out on the Internet, but security experts say their products aren't good enough – none provides complete protection from the many threats out there.

They also tell us that users don't take security seriously. One of their favourite sayings is: *The most likely cause of a car accident is the Nut behind the wheel.* What they mean is that the average business is neglecting security and that most homes leave their front and backdoors wide open.

#### Lost in Space

Many of us would argue that it's not for the want of trying. Malware has spawned too many variants to keep up with, and the jargon of security is an impenetrable jungle (for a rough guide, check this short [GLOSSARY](#)). The next hurdle on this obstacle course is the profusion of security products on offer. We're expected to come to grips with antivirus software, firewalls, spyware detectors, Trojan hunters, rootkit removers, spam filters, ad blockers and parental control software.

No wonder so many users jump into the lifeboats offered by Symantec, McAfee and Trend Micro, whose suites promise to cover the whole terrain. They do that but in the process impose heavy burdens on PCs and users.

(For a no-holds-barred account of one user's struggle with the antivirus mafia, check out [In the Grip of Security](#))

#### The Fine Line between Pleasure and Pain

We're not experts on PC security but our data are precious, so we need the best protection we can find. Some of our friends with Apple Macs used to gloat when we talked about security. They don't gloat as much they used to since Apple released a security update that plugged over two dozen potential exploits in Mac OSX Panther and Tiger operating systems.

Only Linux users can still claim relative immunity, but Windows XP is the operating system on 9 out of 10 PCs. Security wasn't high on the agenda in its design stage and, over the years, XP has been patched more often than the Australian Tax Act. Microsoft claims that Vista is far more secure, but early adopters complain that Vista's *User Account Control* measures are too heavy-handed and spoil their computing pleasure.

#### Mobility comes at a price

With 'always-on' broadband in many homes, our vulnerability has increased. With WiFi on our laptops, we're at risk in on the road as well. To stay out of trouble, we need tougher vehicles, better tools and sharper skills (see [Driver Training](#) for more details).

Even corporate firewalls can't keep all the nasties out. IT managers worry about users who unwittingly load malicious code onto their laptops while away from the office. The malware could come wrapped in a neat screensaver or from peer-to-peer sites offering video clips, or from game sites or those with 'adult content'.

Back at the office, the user walks right past the impressive data centre with its double-brick firewalls and Intrusion Protection Systems, plugs his laptop into the network and infects it in a heartbeat.

*Forrester Research* says: 'Organisations have felt the sting of focusing security on the perimeter while neglecting to secure the end points in the enterprise.' With the number of professionals using a laptops growing by the day, IT Managers are paying more attention to the endpoints

### The price can be crippling

TJX, a retail group based in Massachusetts that turns over \$17 billion a year, didn't pay enough attention to security. Hackers got into the company's network and, over an 18-month period, downloaded at least 45 million credit- and debit-card numbers, which they sold to various gangs who ran up charges using fake cards printed with the stolen numbers. TJX was blissfully unaware of these goings-on and now faces costs that run into several billion dollars.

Analysts say the retailer's wireless network had less security than many people have on their home networks. TJX used an obsolete encryption system (Wired Equivalent Privacy, or WEP) that was easy work for the hackers. Other doors were left wide open, with firewalls and data encryption not installed on many computers in the company's wireless network.

If you rely on wireless LAN technology for your business, here's a complete guide on how to make it secure: <http://downloads.techrepublic.com.com/abstract.aspx?docid=277380>

**[PART 2 – A SNAPSHOT OF CURRENT THREATS](#)**

**[PART 3 – SECURITY LAYERS, A ROUGH GUIDE](#)**