

# Computer Reseller News

ELECTRONICALLY REPRINTED FROM JANUARY 15, 2007

## The perils of portable storage

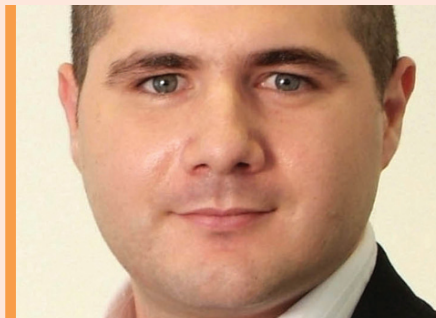
The influx of portable storage devices could lead to danger for companies that are unprepared, argues **Andre Muscat**

» Most companies have seen the influx of digital cameras, iPods and smartphones in the workplace in recent years, but few have taken steps to curb usage.

While enhancing productivity, the truth is that use of portable storage devices can transplant malicious data to a corporate network and give trusted insiders the means to steal valuable corporate data. While most employees do not have bad intentions when they connect a portable storage device to their workstation, the fact is that one employee with a vendetta could bring down the network of a corporate giant.

Many attacks on a network occur when unsuspecting employee devices are infected by Trojans. Trojan attacks can be veiled behind computer games, MP3s or even office applications. Employees face a much greater risk at home when web browsing and downloading are not monitored and regulated. However, when an employee uses a portable storage device both at home and at work, malicious files are easily imported to the workplace.

Malicious code transported via a portable storage device is the most visible threat, but many companies fail to realise the threat to worker productivity



**The control of USB ports can limit unauthorised use and prevent attacks on a company network.**

*Andre Muscat, GFI*

posed by the unauthorised transfer of files. An employee can use company hardware and software to enhance digital photos, play computer games or work on freelance projects. The control of USB ports can limit unauthorised use and prevent intentional or accidental attacks against a company's network.

Although many cases of viruses and spyware uploaded to a corporate network are intentional, the majority of incidents come from unauthorised uploading of

information. Many companies attempt to curb employee use of portable storage devices by implementing policies and rules against unauthorised access to USB ports.

Unfortunately, portable storage devices have become harder to detect and more likely to operate with a computer on a 'plug and play' basis. User-friendly technology means that most employees underestimate the danger associated with connecting electronics to their workstation.

Physical barriers and company policies can be violated. A better solution would be for systems administrators to implement software barriers that stop unauthorised data transfers to and from portable storage devices.

**Andre Muscat is product manager for the network security products division at GFI.**