



## Voice and Data

Date: Friday, 31 March 2006  
Page Number: 12  
Edition: March  
Supplement: Main

Market: National  
Circulation:  
Published: MONTHLY  
Editorial: [email the editor](#)  
Item No: P9750604

Size: 148.28 sq. cm.

### USB creates security risks

A large Australian public sector organisation has identified that more than 1800 breaches of its computer network security occurred in just 10 days' reports. The security specialist Lync Software undertook a detailed audit of the organisation and has quantified the degree of exposure caused by uncontrolled use of iPod, USB (universal serial bus) and other removable media devices within its otherwise highly secured computer environment.

Lync Software managing director Kym Welsby said the results were probably representative of thousands of businesses Australia-wide. "Removable media devices such as iPods, Blackberries and digital cameras get under the radar of network security systems," he said.



"This creates major risks ranging from corporate espionage and business disruption to malicious viruses. Unless businesses can identify and control iPods and other removable media devices, they are leaving a gaping hole in their security systems.

"At the moment, it's like companies are locking the back door with firewalls but leaving the front door wide open, with people coming and going with uncontrolled removable devices."

Lync, an Australian company, has its management and security solutions installed at more than 2000 organisations worldwide including Boeing, Pepsi and Hilton Hotels. Security risks arise from these devices being able to connect undetected to corporate networks, downloading gigabytes of data in a matter of seconds and even introducing viruses.

The Lync software tracked 768 computer users within the organisation identifying the following problems: 39% of users connected to the corporate network with USB devices, 154 different types of device were connected to the network, 1805 files were transferred between the network and the

devices and transferred files including images, music, video, office documents and system files.

Welsby said the organisation had since created a mobile device usage policy to secure its network against accidental or deliberate damage from removable media devices.