

USB Threatens Corporate Information Security

Enterprises globally are grappling with a problem that undermines their heavy investments in Information Security.

The proliferation of highly portable digital devices, such as iPods, smartphones, digital cameras, PDAs (Personal Digital Assistants) and memory sticks has raised a two-edged sword.

While their convenience for the mobile professional is indisputable, these devices largely circumvent the security policies developed to protect the critical business information held by both public and private sector organisations.

In a nutshell, iPods and their ilk have created a gaping security hole that is not addressed by traditional IT security approaches.

Since 2001, USB (Universal Serial Bus) storage devices and memory sticks have replaced the floppy disk and CD-ROM as the device of choice for physically moving files between computers. These units are small, cheap and easy to use.

But this convenience comes at a cost – security. With nearly 100 million USB-type devices sold last year it is obviously massive, although it is virtually impossible to accurately quantify the extent of this security risk.

A recent audit by Australian security software specialist, Lync Software, provides an alarming insight into the scale of exposure within just one enterprise. The detailed exercise used the Lync USB software to monitor the degree of network activity by removable media devices within the otherwise highly secured computer environment.

The 10-day audit identified more than 1800 breaches of the organisation's computer network security through the uncontrolled use of removable media devices.

Lync Software managing director Kym Welsby said the results were probably indicative 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."

Security risks arise because iPods and other music players, USB memory sticks, personal organisers and PDAs, mobile phones and digital cameras can connect undetected to corporate networks. These devices can download gigabytes of data in a matter of seconds and even introduce viruses.

The problem is already bad and will only get worse unless it is addressed.

Gartner estimated that 2005 would produce 85 million shipments of USB storage devices with an average capacity of 462Mb*. By 2010, that will grow to 168 million shipments of USB storage devices with an average capacity of 4.8Gb.

As a result of the unsecured and unmonitored use of USB-type devices, organisations face three major risks:

1. · Data theft (unintentional and deliberate)
2. · Introduction of malicious code
3. · Increased support costs.

Mr. Welsby said businesses needed to recognise the threat caused by the proliferation of mobile devices on their networks. "The unique nature of these devices, both from a technological and usage viewpoint, create security and management problems that fixed IT assets do not experience," he said.

"Mobile devices are often outside the protection of the network and inexpensive devices are regularly brought into a network without the knowledge of IT management. It is easy to download sensitive information without the IT manager being any the wiser

"At the same time, malicious software code can be introduced to the network without having to go through the enterprise firewall. In addition to security risks, support costs can rise due to the technological immaturity of these devices and conflicts with existing systems.

While organisations are understandably sensitive about disclosing security details, numerous examples have appeared of security breaches caused by the mismanagement of mobile devices.

In 2005, a government health agency that stored confidential patient information on a series of Access databases employed an independent IT contractor to undertake enhancements to a database. The database contained patient data, detailing names, addresses, disabilities and prescribed treatments.

The entire database was copied to a USB drive and installed on to the contractor's home PC. The agency had no way of stopping the removal of the database from the network and no way of knowing the highly sensitive data entered the public domain.

In another case, a BlackBerry that belonged to a former Morgan Stanley executive sold on eBay for \$15.50 in August 2003.

The buyer discovered that the device – which had been sitting in a desk drawer without batteries for months – still contained hundreds of the firm's confidential emails as well as personal information about the former owner.

Although Morgan Stanley had a policy stating that mobile devices were to be returned to IT for data cleansing, no one followed up when the executive left the company. While the email account was deactivated, old emails remained intact on the device.

A measure of the extent of this problem occurred in November 2005 when Lync Software undertook an audit of mobile device usage on a large Australian organisation's network. The company used its software to track 768 computer users for 10 days. Findings included:

- 39 per cent 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
- Transferred files including images, music, video, Office documents and system files.

Before this audit, the organisation was unaware of who used USB devices and what information was transferred from the network to these devices. It was also unable to identify what potentially malicious files were brought onto the network from removable media within the firewall.

The audit involved the installation of the Lync USB software to monitor removable media devices connecting to the organisation's main networks. USB storage devices include flash drives and removable hard drives. The smartphone category is comprised entirely of Symbian-based phones.

In addition to discovering what devices were connected to the network, Lync USB reported information of file transactions between the network and these devices. Details included the source location of files transferred to devices; the name of transferred files, the type of files transferred and the size of files transferred.

The report provides a comprehensive audit trail of information flowing to and from mobile devices, a vital safeguard for organisations that hold sensitive data.

Mr. 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. "This has secured their network against intentional or unintentional data theft and potentially harmful files entering the network, bypassing their corporate firewall," he said.

After the audit report, the organisation identified information security as an essential enabling mechanism for information sharing and initiated a project to mitigate risk and to govern USB device usage across the enterprise. Potential outcomes include:

- Changing the way different type of users will use USB devices,
- Allowing and disallowing certain kinds of USB devices, and
- Allowing and disallowing certain types of files to be transferred between USB devices and the network.

Globally, there are varying privacy laws and compliance regulations. The effect of these laws and regulations is to create a significant risk if personal details, sensitive corporate data or secret government information ends up in the hands of unauthorised third parties.

As well as the threat of litigation, fines or other undesirable legal consequences, an organisation's reputation can be jeopardised, causing customers or partners to lose faith in dealing with the organisation.

This is particularly important in areas such as financial markets and government and health care.

To address the problems caused by uncontrolled mobile devices, Lync Software and its US partner Layton Technology have collaborated to develop DeviceShield, a software package that identifies and controls removable digital devices.

DeviceShield can be downloaded and installed within minutes, providing a centralised management console to control removable media devices operating on a computer network. As well as identifying when removable media devices connect to computers on the network, DeviceShield can control whether data is downloaded to the device or copied from it.

DeviceShield costs from \$695 for a 50-seat licence. A fully functional version of DeviceShield, which runs for 14 days, can be downloaded from www.lyncsoftware.com.

About Lync Software

Lync Software is the Australian developer of innovative management and security solutions that enable enterprises to reduce the risks created by the proliferation of removable media devices such as iPods, PDAs, smartphones and digital cameras. Lync's world-leading software is already installed at 2000 corporations globally including Alcoa, Boeing, Hilton Hotels, Heinz, Lockheed Martin, Pepsi and Time Warner. Founded in 2000, Lync Software markets its software through an international reseller channel and OEM partners.

* Source: Gartner – Market Trends: USB Flash Drives, Worldwide, 2001-2010, 1 September 2005