



This feature article outlines the risks you "have faced since they were introduced" through use of USBs as storage devices within and throughout your organisation.

".....allowed the two men to copy 1,048 computer files of technological data and 17 books on managerial knowhow simply with USB flash drives.

Prosecutors, quoting a company statement, said the theft could cause some \$US3.05 billion in lost sales and price cuts over the next five years."

Is Your Data leaking.....?

is a feature article, in the
Managing Clouds and Moving Goalposts ©
series of "Management Focused" articles
by PCProfile <http://www.pcprofile.com>



INTRODUCTION

Everyday, in every organisation around the world, business and government sites are using USB drives as a means to store and relocate data files. There are literally billions of these USB storage devices in use, everywhere!

Maybe you haven't yet considered the risk of using these devices, that have been in use since 1998.

If not, then now is a good time to take stock of the data that might be leaving your building, maybe right under your nose!



PREVENT DATA THEFT

From PCs to digital cameras to USB flash memory to PDAs to set top boxes to mobile phones to consumer electronics, the USB connection has provided the seamless connectivity solution to enable high speed, driver-less interface between everyday technology devices.

Standard USB devices that in 2001 had around 8MB of storage space, are currently storing around 64GB to 80GB of data in 2007, which is usually more than the average PC hard drive storage capacity after taking into account operating system size!

Through their popularity, ease of use and availability, USBs have pushed the security perimeter beyond safe limits and need to be considered a significant threat unless you have already done so.

If you are running a business and have employees working and communicating remotely, then you should already have in place sufficient levels of security and protection to cover sensitive data on portable devices such as laptops, and PDAs. This is to prevent against loss or theft of the physical asset.

USBs AT WORK



But have you considered that there are also more benign risks posed with USBs, thumb drives, and even iPods in every day use within your office and business?

Unfortunately, the uncontrolled use of USB devices as storage media means that files may be escaping out your front/back doors of your business containing images, music, video, office documents and other sensitive files.

USBs are one of the most widely used means of transferring data files to and from the office when staff are working off site or moving between locations. The latest breed of USB3's has software and user preferences embedded within them and coming soon to a desktop near you will be Wireless USB devices!

Using USB as a data storage medium, whilst extremely convenient and portable (and concealable) pushes the security boundary further. With USB3 for instance you have no way of knowing what the embedded software and user preferences are capable of doing. e.g.; is it going to extract data files, user information, sensitive data or leave behind a Trojan or root kit that will cause damage at some later point in time or be activated on some event.... against your system?

Access to your systems needs to be controlled and many organisations' spend significant

amounts of money and effort securing the boundary zone against virus attack, spam, malware, through firewalls, anti-virus software and employ security access through password/logon controls etc and the like to prevent external intrusion to systems. This usually is enough to cover the external perimeter area, as long as it is maintained up to date against emerging threats.



UNDER YOUR NOSE

But what about “the inside the walls aspect” where data may leak out the door?

Have you considered the significance of the use of USB drives and MP3 players, iPods etc within your organisation?

It’s now fairly easy to pick up iPods and MP3 Players that allow around 80GB of data storage area for recording music/videos etc for end user listening pleasure but as these devices come with a USB port connection, they not only allow music to be heard quietly at the desktop without upsetting those around you, but also can be used to drag and drop data files to, such as confidential data, customer lists, price lists, credit card details, personal information, product designs etc etc.

The 6th Generation iPod Classic can store between 80GB and 160GB of data in hidden folders on the storage media embedded within the device. This device can be read and written to by Windows XP and Vista based systems. Source

<http://en.wikipedia.org/wiki/iPod>

Statistics vary widely on USB shipments worldwide with an estimated 3billion USB 2 units shipped worldwide between 2003 and 2007. TechWeb.com

<http://www.techweb.com/wire/mobile/186700631> reported in April 2006 advising “Wireless USB, anticipated to begin to be widely deployed in the third quarter of 2006, will boost USB shipments from 1.4 billion per annum in 2005 to 2.8 billion per annum in 2010”.

With these sorts of volumes of USBs in circulation this means that the threat inside the walls needs to be monitored and controlled in a manner that still allows you the ease of convenient access to data for operational efficiency.



EASY TO USE – EASY TO LOSE!

Ease of use? One enterprising US consultant claims to have been paid (by the customer organisation) to configure some USB devices as an in-house security survey and left these USBs lying around in the local customer car park. The software installed by the consultant (with company permission) monitored user activity and sent details back to a central location when the users picked up these devices laying in the workplace car park. Needless to say the end result justified tightening up the use of devices in the area, even if the approach taken was somewhat unorthodox. For obvious reasons we can’t name the organisation or the consultant, but it does illustrate the mindset you need to overcome. Ask yourself the question – what would you do if you found a USB drive in a restaurant, bus/train, car park or a lift? Most people instantly react by “plugging it in” to see what they can locate on the USB. Too late, if the USB had Trojan software such as outlined here.

USB is prominent in the following devices: Personal Computers, MP3 Players, iPods, BlackBerries, PDAs, Digital Cameras, Set Top Boxes, Printers, Scanners, Mobile Phones, Flash Memory, Other PC Peripherals, and Communication Devices.

If your business is using or relying on sensitive private and third-party information, bank account and credit card details, medical records, business documents, designs, drawings, software, and other personal information and these are leaking out the backdoor via USB

devices then the legal liability arising to the enterprise for not properly securing the data can be very significant.

THE BOTTOM-LINE



The use of USB storage devices of all types, through the actions of your employees as trusted insiders, including consultants, contractors, vendors, and partners - must be actively managed, audited, and monitored in order to protect sensitive data.

The Bottom-line according to PCProfile?

Now is the time to make sure that you assess your position across the enterprise, mandate a policy of USB usage and compliance by ensuring that end users can use approved USB devices in your systems and that data access controls are in place to monitor activity.

You need to start with a clearly defined policy about the use of USB data devices within your organization. If you are employing any software agents to track the usage make sure employees know about the device checking being done and explain why it has been implemented.

PCProfile Tip - The best tip we can give you is to make sure that you understand what is happening, make sure your users understand the implications and that you take control of the whole process so that you can manage this situation rather than the situation managing you.

USB Data Theft in the News

BBC NEWS | Technology | Warnings over USB memory sticks - Windows Internet Explorer

http://news.bbc.co.uk/2/hi/technology/4946512.stm

Google Search Site Google Earth Google Earth Button Gallery

Snagit Web Search Your Big Island Vacation Rental Home Awaits You - Ohia Plantat

Calling ID

Home News Sport Radio TV Weather Languages

UK version International version About the versions Search

Low graphics Accessibility help

BBC NEWS WATCH One-Minute World News News services Your news when you want it

News Front Page Last Updated: Thursday, 27 April 2006, 08:07 GMT 09:07 UK

E-mail this to a friend Printable version

Warnings over USB memory sticks

By Mark Ward
Technology Correspondent, BBC News website

Smart phones, iPods and USB memory sticks are posing a real risk for businesses, warn security experts.

Just over half of companies take no steps to secure data held on these devices, found a UK government-backed security survey.



US military secrets were found in USB sticks on sale outside airbase

SEE ALSO:

- Data dangers dog hard drive sales
12 Sep 05 | Technology
- The rise of the keyring drive
28 Apr 03 | UK
- Stones release memory card album
28 Sep 05 | Entertainment
- Intel deal for iPod memory chips
21 Nov 05 | Business
- Afghans selling US army 'files'
12 Apr 06 | South Asia
- US buys back stolen Afghan files
15 Apr 06 | South Asia

RELATED INTERNET LINKS:

- Secure Wave

Source <http://news.bbc.co.uk/2/hi/technology/4946512.stm>

Ex-Boeing worker accused of stealing documents - Network World - Windows Internet Explorer

http://www.networkworld.com/news/2007/071307-boeing-employee.html?page=1

Google cyspl Search Site Google Earth Button G

SnagIt

cyspl Bank Loans For Small Businesses - Search lenders, fir

CallingID

"data thef... Enterprise... dr New Soft... Nw Ex-Boei... x

NETWORKWORLD

Monday, October 29, 2007

sterling commerce An AT&T Company

HOME

RESEARCH CENTERS

Security

Anti-Virus / Spyware / Spam

Compliance & Regulation

Firewalls / VPN / Intrusion

NAC

Services

Cisco Security Watch

Microsoft Security Watch

+ LANs & WANs

+ VoIP & Convergence

+ Network Management

+ Wireless & Mobile

+ Software

+ Data Center

+ Small Business Networking

Cisco Subnet

Microsoft Subnet

Security

Whitepapers Guides and Reports Webcasts Videos Buyer's Guide

NetworkWorld.com > Security >

Ex-Boeing worker accused of stealing documents

Gerald L. Eastman allegedly stole documents that could cost Boeing up to \$15 billion

By [Jon Brodtkin](#), Network World, 07/13/07

[Comments \(13\)](#) [Print article](#)

Short of strip searching employees every time they walk out the door, there's probably nothing [Boeing](#) could have done to prevent the alleged [data theft](#) that has a former employee facing criminal charges, security expert [Bruce Schneier](#) says.

Gerald L. Eastman, 45, was accused this week of 16 felony counts of first-degree computer trespass for putting highly sensitive files onto a USB thumb drive and trying to leak them to newspaper reporters,

Other stories on this topic

Disney Movie Club members victimized in latest data-breach horror show

ChoicePoint details data breach lessons

06/11/07

Top 10 st

MOST-

1. Netw
2. Unlin
3. Storr
4. Senz
5. Vonz
6. Cisc

IT TOO

Steelhea Real-tim

Source <http://www.networkworld.com/news/2007/071307-boeing-employee.html?page=1>

Techno-secret theft - Windows Internet Explorer

http://www.tradingmarkets.com/site/news/Stock%20News/708913/

Google "data theft" usb Go Search Site Google Earth Google Earth Button Gallery

Snagit Web Search Bank Loans For Small Businesses - Search lenders, find mortgage deals

Calling ID

"data theft" usb - Goo... Techno-secret theft Mobile security is mor...



Interbankfx Earn up to **\$2500** when you trade Forex

>> click for details <<

POWER RATINGS (for Traders) Enter Symbol GO SEARCH GO PowerRatings FREE TRIAL TradingMarkets FREE

Home TM PowerRatings TM Products TM Stocks TM Options TM Forex TM E-minis/Futures

Featured Trading Products

5x5x5 Portfolio Method

Are you a momentum trader? How would you like to own a momentum trading method that has had double-digit or triple-digit returns every year?*

FREE PRESENTATION
Tuesday, Oct 30, 04:30 PM EDT

To attend this free presentation [click here](#)

*Based on simulated trading results.

Raptor II TRADING SIGNALS

Since 1995, Raptor II has gained on average 11.26% per winning trade within 8 trading days.* We are now pleased to offer you the opportunity to license the Raptor II Signals on a monthly basis.

[More Info >>](#)

▶ Start Your 14-Day FREE TRIAL

See All of Our Trading Products

STOCK NEWS [More News: Top Stories | Stock Alerts | All Trading News](#)

Techno-secret theft

Wednesday, October 17, 2007; Posted: 12:43 AM

Oct 17, 2007 (Asia Pulse Data Source via COMTEX) -- [PKX | charts | news | PowerRating](#) -- POSCO is a big steel maker, ranked third or fourth in the world. It employs more than 13,000 workers at its Pohang and Gwangyang steel mills. Two men who worked for POSCO's R&D arm until last year were arrested last week for stealing important technologies and selling them to a competitive Chinese company.

The theft of core technologies from an industry leader has grave consequences.

Prosecutors, quoting a POSCO statement, said the theft could cause some 2.8 trillion won (\$3.05 billion) in lost sales and price cuts over the next five years. China's steel industry is known to be some five years behind Korea's in terms of overall technological standards. This gap could narrow significantly because of the crime.

More Breaking News about PKX

- » [SK NETWORKS FINISHES STEEL-PROCESSING PLANT IN CHINA](#)
 - » [Steel to attract nearly Rs 3 lakh crore investment in 5 years](#)
 - » [STOCKS - SEOUL SHARES FALL AFTER STRONG START - OCT 26, 2007](#)
- [Click here for More News >>](#)

More Resources for PKX

- » [PowerRatings \(for Traders\)](#)
- » [PowerRatings \(for Investors\)](#)
- » [Quotes & Charts](#)

Source <http://www.tradingmarkets.com/site/news/Stock%20News/708913/>



Published by PCProfile.com

Worldwide Copyright Notice

Copyright © 2008 PCProfile trading as Rob Harmer Consulting Services Pty Ltd ABN 77 035 134 400 All rights reserved worldwide.

Guidance For Publishers

Publishers are encouraged to publish this report as free content resource in accordance with the following guidelines:

- 1) Articles must be published "as is" (unedited);
- 2) Articles must be published with the author's bio paragraph and copyright information included;
- 3) URLs listed should be set as hyperlinks, with no redirection;
- 4) Whenever possible, authors should be notified of intent to publish;
- 5) This Published Article cannot be used in spam communications or sold;
- 6) PCProfile prohibits the use of copyrighted material in a manner that violates the copyright owner's rights;
- 7) Publishers who violate copyright law are legally liable and subject to possible fines under Copyright Laws worldwide.

Disclaimer

The content of this report is provided for informational purposes only as "guidance notes" and for redistribution as outlined in the "Guidance For Publishers" paragraph and Copyright Notice above. PCProfile does not represent that all technology aspects have been outlined as a complete position and does not accept any responsibility or liability for the use or misuse of the content of this report or reliance by any person of the publisher's contents.

About the Author - PCProfile is an Australian based company located in Adelaide with over 30 years practical computing experience in small, medium and large enterprises and offers managers and business owners in SMEs, and SOHO businesses practical tips and advice on how to get the best out of the technology used by your SME/SOHO business.

An advertisement for PCProfile. It features a man in a white shirt and tie sitting at a desk with a laptop, looking stressed with his hand on his forehead. The background is a light blue gradient. Text overlaid on the image includes: "Struggling with technology?" in large, bold, black letters; "PCProfile offers practical technology tips aimed at helping you use your PC business systems more efficiently." in smaller black letters; and the PCProfile logo and website address "www.pcprofile.com" in the bottom left corner.

Other Self Help "Tips and Tricks" Tutorials and feature articles on management aspects of software piracy etc are available at;

www.pcprofile.com/features.htm

PCProfile also runs seminars on technology topics for SME and SOHO business owners.

www.pcprofile.com email enquiries@pcprofile.com Mobile 0448 650 227

Seminars www.pcprofile.com/seminars.htm