

### **"It's 2004 and Year 2000 is about to hit us again!"**

First reactions on reading the headline above will make you think we had "lost the plot, totally". Your reaction is likely to be "OH, NO", not another "the sky is falling" message, we had that detail all through the years 1997, 1998, and 1999 which is now 4 to 5 years ago! Before you turn off, please read on as there are issues that CEOs, Managers, Directors need to be made aware of to reduce their personal risk.

So, why write an article in 2004 about the Year 2000 issue?

### **The reality is there a knock-on effect, which will appear this year that needs to be considered when it comes to PC's!**

"The Year 2000 was a fizzer" according to many (yet, the real systems that did break didn't get publicised did they?) and as a result many mega-millions of \$ were spent on both the PC hardware and the software to make systems "Year 2000 compliant".

This was to overcome legal issues that might arise as a result of failure due to Y2K, and businesses and government systems could continue unaffected without disruption. The decisions made at that time were a perfectly valid risk reduction exercise, albeit costly, but necessary.

### **So why bother start talking about Year 2000 again?**

This article is reality check on what is about to occur in 2004, right around the world.

The technology pundits are predicting that many organisations will be spending some of their IT budgets this year on replacing computers.

Many of the PC's that were purchased in 1999 have passed their "use-by date" in many cases and many organisations are considering hardware refresh, or replenishment as a means to keep up-to-date with latest technology for maintaining their competitive advantage. This is a normal, business case driven, risk reduction strategy.

### **However, there are some unforeseen risks looming.**

Where you are the Owner, The Managing Director, the Chief Executive Officer of any organisation (business, government, semi-government or not-for-profit) that is facing the budgetary pressures and decisions to replace hardware, there are some issues surrounding disposal of the OLD PCs that you need to be made aware of, as these have taken on a new dimension in recent months, with the risks that you face, increasing.

### **Approval of NEW for OLD PC changeovers**

When considering or approving any PC replacement program, has your IT department or Computer Manager or Consultant, or

Vendor given you explicit details on what is to be done with the OLD PCs? You may have already asked questions such as:

Are these old PC's to be?

- Decommissioned, stripped down and used for spares?
- Reformatted and used elsewhere within the organisation?
- Given away to charity or not-for-profit use?
- Traded-In to the vendor selling new systems?
- Sold at auction?
- Sold to staff for home use?
- Dumped at the local tip? (An environmental disaster if they are!)
- Or sent to a recycling vendor for refurbishment and then on sold later for a margin?

It really doesn't matter what the answer is to the above questions or which path you choose (some are much better than others), although we DO NOT advocate tipping them on the rubbish heap for environmental reasons!

### **BUT, have you asked ONE KEY question?**

Will these PCs be cleaned of any data before they leave our asset controller?

Now its about here that the IT experts who work for you, will all jump in and say, "doesn't matter, we haven't got time for that, we'll just delete the directories and files or we'll just format the hard drive and reissue it!".

### **NOW ASK THE NEXT QUESTION THAT IS VITAL!**

**Before disposing of any PC can they provide a confirmation certificate that all data has been totally removed and destroyed?"**

We'd like to be there when they answer this one!

### **"A BLUNT MESSAGE TO THE DIRECTOR, CEO, MANAGER - THIS IS NOT GOOD ENOUGH!"**

The reality is that current methods (without using specialist tools) cannot do this for you. Hence there is always a risk, that data is NOT cleansed from the system. Can you afford this risk?

The answers given by the IT experts, will generally not be good enough in terms of ensuring that data files are cleansed from the PC based system. There are ample Forensic tools on the market that can recover any formatted drive or unerased data. It's a fact! We can point you to the newsgroup community that specialises in this area and the vendors in this field are constantly refining their techniques of data recovery.

**BE VERY CLEAR about the RISKS YOU FACE!**

**IN ALL CASES, YOU MUST**, and this is underlined, in bold, italics, and redlined for embedding on your memory, forever, **YOU MUST ENSURE** that each and every PC is cleansed in such a way that ALL data is destroyed and removed from "the system".

Think about the following that applies in Australia (and is appearing in other places around the world);

In Australia, The [Federal Privacy Act](#) 1988 contains eleven [Information Privacy Principles](#) (IPPs) which apply to Commonwealth and ACT government agencies. It also has ten [National Privacy Principles](#) (NPPs) which apply to parts of the private sector and all health service providers.

The following two clipped segments were extracted from; <http://www.privacy.gov.au/business/index.html> and <http://www.privacy.gov.au/business/infosh/index.html> and Guideline 6-2001 Security and Personal Information ([HTML](#) 16.9 kb [Word](#) 46 kb or [PDF](#) 19 kb).

**For Small Medium Enterprises, (SME's) PLUS all Medium to Large sized Commercial Organisations**

**National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000)**  
**4. Data security**  
 4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.  
 4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2

**For Government Sector Organisations**

One key principle applies to ALL Government sector organisations including Not-For Profit groups in Australia that has direct relevance to this topic;

**Information Privacy Principles under the Privacy Act 1988**  
**Principle 4 - Storage and security of personal information**  
 A record-keeper who has possession or control of a record that contains personal information shall ensure:  
 (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and  
 (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

*The Privacy Act 1988* (Commonwealth of Australia) ("the Act") does, both allow and afford, organisations and industries to have and to enforce their own privacy codes that continue to uphold the privacy rights of individuals while allowing some flexibility of application for organisations.

## Where is "Personal Data" stored?

Besides the obvious places like, My Documents and other readily viewable directories/folders etc, data can also be stored and accessed as follows;

<ul style="list-style-type: none"> <li>■ Some Cookies contain data about passwords, account numbers etc</li> <li>■ The Registry! The Registry is never cleaned in the manner you expect and often residual data contains personal information including password files</li> <li>■ PWL is the password file used for Microsoft Passport</li> <li>■ Recent documents lists</li> <li>■ History files and folders</li> <li>■ Swap files</li> <li>■ Vcards</li> </ul>	<ul style="list-style-type: none"> <li>■ E-mail contact lists</li> <li>■ E-mail headers and footers</li> <li>■ Address books</li> <li>■ Phone lists</li> <li>■ Contact databases</li> <li>■ Temp folders</li> <li>■ Encrypted files</li> <li>■ Digital signature certificates</li> <li>■ Cached web page areas</li> <li>■ Backup folders</li> <li>■ Hidden folders</li> <li>■ Batch and Txt files specially written by users</li> <li>■ Some INI files</li> <li>■ Some DLL files, and</li> <li>■ Folders with names like c:\\$NtUninstallKB828035\$</li> <li>■ or d:\{B3C1B200-8F14-4C49-96D3-67425AD59914}</li> </ul>
--	--

This means that VERY SPECIAL ATTENTION needs to be considered to ENSURE that ALL DATA on any PC is REMOVED and THOROUGHLY CLEANSED in a manner that affords the Owner, The Managing Director, the Chief Executive Officer of any organisation (business, government, semi-government or not-for-profit) the "duty-of-care" protection against being held liable for misuse or mishandled private information, that has been stored on PCs that were a part of your asset base and now no longer required.

In Australia we have had the occasional press article about PCs that have been 'sold at auction', "found at the tip etc" or in second-hand dealers hands that have had readily accessible (uncleansed) amounts of personal data. Some data has been reported from police files, other has been health and personnel and government records and so on.

## In 2004, YOU CAN NO LONGER AFFORD TO TAKE THIS TYPE OF RISK!

As Directors, CEOs, Managers etc you need to ensure that your organisation keeps a permanent written log of all PCs that have been "disposed of" no matter what method of disposal has been used.

This log MUST provide you with the evidentiary certificate for every PC to demonstrate that all data has been removed BEFORE shipment/disposal.

Ask your IT personnel the following question, "When disposing of PCs can they provide you with a confirmation certificate" that contains detail such as;

■ Computer ID label	■ System UUID
■ CPU ID label	■ User identification
■ CPU serial number	■ Number of overwrite passes on data cleansing
■ CPU speed	■ Date and time of start and finish
■ Hard drive name	■ Number of errors incurred during cleansing
■ Hard drive capacity	■ Confirmation erasure code
■ Hard drive serial number	
■ Motherboard serial number	
■ System manufacturer	
■ System name	
■ System serial number	

We can provide you with a report containing all the above detail in HTML, Text and Excel formats that is TOTALLY Tamper PROOF as a written certificate result for each PC cleansed!

How else are you going to demonstrate that you have satisfied "the data security and privacy requirements" under the Australian Privacy Act?

Besides, it's just plain commonsense not to throw away Corporate information so competitors can access your files. Or have they already got your data, customer lists, and Intellectual property from some PCs sold at the last auction?

#### CAVEAT ONE.

Any PC that is the subject of a fraud or forensic investigation needs to be set aside from this process and quarantined so that any fraud activities under investigation are not jeopardised by this process.

#### CAVEAT TWO.

Don't forget that there are external peripheral devices attached to these PCs such as USB drives, Memory cards, CryptoCards, ZIPDrives, SmartDrives, and so on that have "data stored" which also needs cleansing. There are PDA's PalmPilots and even new generation Mobile Phones that present similar risks that require slightly different treatment before disposal.

#### TO REDUCE YOUR RISK - ADOPT BEST PRACTISE

1. Quarantine from sale / disposal any PCs that are the subject of a Fraud investigation
2. Backup ALL Corporate data from unused PCs to servers or CDs PRIOR to sale/disposal
3. Cleanse the PC with a SECURE Cleanser that gives a comprehensive written report of the state of cleansing, PC by PC
4. Dispose of the PCs in an environmentally friendly and safe manner
5. File all certificates in a secure area as a record of disposal of the asset. This is YOUR PROOF of Safe Destruction.

## The Bottom Line Message?

**To REDUCE YOUR RISK, YOU MUST ENSURE ALL PC's leave your hands ABSOLUTELY CLEANSED OF ALL DATA and that you have records to PROVE it!**

**If you want to know more about HOW you can REDUCE your risk TODAY, please contact us at the address below.**

E-mail [robharm@pcprofile.com](mailto:robharm@pcprofile.com)

Web site <http://www.pcprofile.com/>

"Managing Clouds and Moving Goalposts"

Copyright © 2003-2004

Rob Harmer Consulting Services Pty Ltd

ABN.77 053 134 400

P.O. Box 196 Modbury North Sth Australia 5092

PCProfile is based in Adelaide, South Australia

Phone +61 8 8263 0222 Fax + 61 8 8265 1961

Time zone GMT +10:30

### Why "Managing Clouds?"

*"As soon as you see them forming they change shape and form again, sometimes turning into vapour, other times dumping rain all over you! .....and you really can't manage them at all!"*

The role of any manager is complex and difficult and with rapid changes taking place all around you it's difficult to know where to find practical advice on "how to manage" these changes. This is especially true when you think you have it all under control then find the rules change, again, and again.

This is when it's more like "Moving the Goalposts"!

This is the 1<sup>st</sup> in a series of Practical Topics that have relevance for Managers in 2004

Written Permission to reprint this article is available by contacting the author by e-mail; [robharm@pcprofile.com](mailto:robharm@pcprofile.com)