

Information Overload

Issue 76, June 2009

Welcome:

Welcome to the June edition of IEA's e-zine "Information Overload".

The myth of the paperless office is still evident with every organisation regardless of size creates vast quantities of information every day. Whilst some of it is born digital and will remain that way, a lot more is paper bound. As you are aware, the reason we can drown under tonnes of paper is a simple one. No longer are we constrained by the typing pool and the number of legible copies we can make using carbon paper. For the younger generation of readers out there – we are talking BC – as in "Before Computers" when some desks had a typewriter and other people relied on pads of paper and a pen to write their reports, letters, memo's and were handed to the typists to transcribe. Yes things have moved on since the days BC. For starters we have access to photocopiers which can churn out thousands of copies of a document within minutes. However, this edition of Information Overload is not overly concerned with the paper based records we have lurking in cupboards under the stairs or the warehouses filled with un-sentenced boxes of files and documents, rather the documents and files that reside on our computers.

With technology comes a new set of problems. "BC" we had poor handwriting and many drafts to keep typing and re-typing to get right. We were limited by the speed and accuracy of the typist, copious amounts of white-out and the ability of the originator to write legibly and have clarity of thought at the time of composing the document.

With computers of course we have the opposite. We can produce as many copies of a document as we want. They can be edited and re-written to our hearts content without thought to drafts, revisions or printing out a final copy. We can also delete those errant bits and bytes at the touch of a button – or two, or copy them onto a portable storage device, which as you can imagine creates another set of problems relating to record keeping and the security of our information.

We hope you enjoy reading. Have a great week.

Lorraine Bradshaw
Marketing Coordinator and Projects Manager

In this issue we will look at:

- Portable Storage Devices
- Privacy and security of information
- Contract clauses and the consultant
- A Thought to ponder

© IEA 2009. All rights reserved. You are free to use material from the Information Overload newsletter in whole or in part, as long as you include acknowledgement of source.

Information Enterprises Australia Pty Ltd
Unit 4, Upper Level, 201 High Street, FREMANTLE WA 6160
Tel: 08 9335 2533 Fax: 08 9335 2544 e-mail: training@iea.com.au

Portable Storage Devices

“A Portable Storage Device (PSD) is defined as a small, lightweight, portable, easy to use device, which is capable of storing and transferring large volumes of data. Common PSD’s include portable external hard drives, CDs/DVDs, USB Keys, laptops/notebooks, personal digital assistants (such as Pocket PC, Palm, Blackberry), and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones).”

Australian Government Office of the Privacy Commissioner.

Public Sector Information Sheet 3 – Portable storage devices and personal information handling

As we mentioned in the introduction, we don’t have to lug pads of paper or cumbersome typewriters around with us anymore. Whilst some of us will still carry laptops, more people are relying on portable storage devices to transfer information, and therein is the beginning of the problems we face.

There have been many news reports over the years of PSD’s being lost, stolen and left behind in taxi’s and hotel rooms. The more damaging the information contained on the PSD the more we tend to hear about them (as we all know “bad news sells”). For anyone who has used a PSD will know how easy it can be to lose something as small as a thumb drive, so why do we rely on something so small to transfer our important information?

Privacy and Security of Information

There are many aspects to the privacy and security of our information. Perhaps one of the biggest issues with using a PSD is that unless the device is security enabled or encrypted, if we lose or have stolen the device, the information contained on it is vulnerable. We may have firewalls, passwords and dragons guarding the gate on our computers and servers, but our information is still vulnerable. You have:

- Deliberate removal of information and
- Accidental removal (deletion) of information

There are several types of deliberate removal of information. There is a legitimate need to copy files and documents and take them away from the office environment, and there is removal of information for malicious intent.

Industrial espionage may sound like something out of a Tom Clancy novel, but it is still as prevalent today as it was back in the “cold war” days. Information is power and if you can shorten the research phase for getting a new product to market by “acquiring” your competitor’s information (and not get caught) then you can potentially save yourself millions of dollars.

Getting around this kind of theft is difficult. A good “thief” would be one who has never been caught and whose background would be clear – so a police clearance would not be any good. Whilst you can secure your information by ensuring documents cannot be emailed outside the organisation and thumb drive slots have been disabled it doesn’t stop people taking a photograph of the document using their own camera, unless you also ensure these kinds of devices aren’t allowed on-site. Given most MP3 players and mobile telephones can

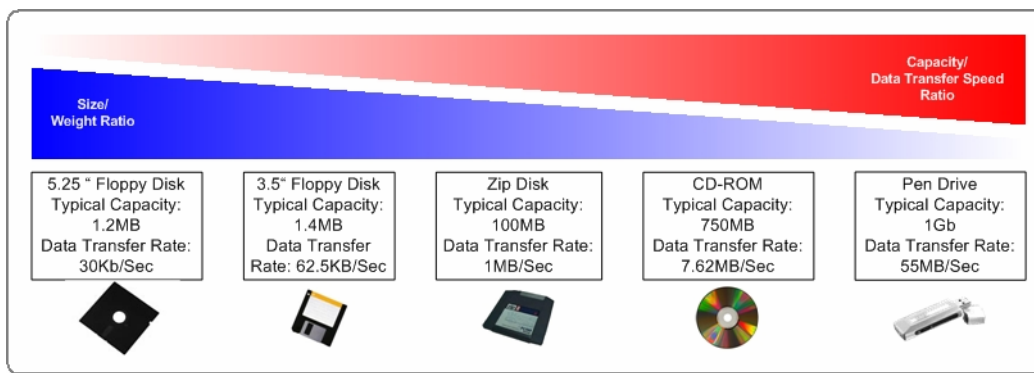
© IEA 2009. All rights reserved. You are free to use material from the Information Overload newsletter in whole or in part, as long as you include acknowledgement of source.

Information Enterprises Australia Pty Ltd
Unit 4, Upper Level, 201 High Street, FREMANTLE WA 6160
Tel: 08 9335 2533 Fax: 08 9335 2544 e-mail: training@iea.com.au

hold far more data than most thumb drives – can we ever hope to secure our information? But who has the time or patience to search everyone, every single day? Then you have the disgruntled employee who decides one day to copy the payroll file over onto their PSD of choice so they can cause untold damage to the people “they” have deemed to have wronged them.

“According to the Ponemon Institute, 59% of people who lost their job admitted to taking confidential company information with them either on DVD or using USB drives.”
<http://www.gfi.com/endpointsecurity>

Whilst some theft of information may be a spur of the moment thing by a person, imagine just how much a person can remove over the course of a week, a month or a year? Plug in an external hard drive – and you have a recipe for disaster. Given the capacity of modern PSD’s you could easily lose all your information.



<http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf>

The main problem associated with PSD’s is this – they can bypass the external firewalls of most organisations. Whilst the average person should not be able to gain access to your files from an external location (unless they have been given permission of course), simply taking a PSD into the organisation and plugging it into a computer hard drive tends to get around that problem quite easily. And whilst information can be removed from a computer quite easily using a PSD, so information can be introduced.

Whilst the average person would not deliberately inflict malware onto their organisation it can and does happen all too frequently. How many of you take CD’s into work to play on your work’s computer (well you have to listen to music to make the day more bearable!!) all a CD production company or music producer has to do is add some code to the disc and they can – in a simple example – be emailed whenever the CD is played. Add the deliberate infections from the same disgruntled employees who want to ensure the problems continue after they have left and you can see why it becomes essential to have policies and procedures in place to cope with these kinds of issues.

But what of legitimate uses? Take for example people who do need to work from home on occasion. Or the organisations that have employed the services of a consultant who will need access to information in order for them to undertake their role.

Contract clauses and the Consultant:

If you use outside consultants and need to share information with them (and what would be the point if you didn't!) it is essential you get a non-disclosure agreement signed. But like we have covered in the previous sections – enforcing this can be difficult, and it comes down to a matter of trust.

The contract condition should stipulate that the consultant should return all material / files back at the end of a project. Bear in mind however, copies can be kept on personal computers (which may be conveniently forgotten about).

Perhaps one of the only ways around these kinds of issues is to ensure you adopt the “mission impossible” way of dealing with information after it has been read. Whilst a rather frivolous idea, passwords can be time and location sensitive – allowing access to material (whilst onsite) for a limited time in a limited way. Ensuring the machine being used does not have internet and email access and disc and USB drives disconnected – may ensure your material (in this instance) stays where it should.

But given our previous comments on how easy it is for insiders to compromise the organisation's information it does make you question why you would bother.

With many thoughts

Lorraine

A Thought to Ponder:

“98% of all crimes against companies in the U.K. had an insider connection.”
Scotland Yard

Your comments and suggestions on the subject of this newsletter are most welcome. Or if you would like to see other issues covered in future editions, please email me at training@iea.com.au. Please feel free to pass on this newsletter to your colleagues' friends and associates. To subscribe they should send an e-mail to training@iea.com.au with “subscribe newsletter” in the subject line.

If you would prefer not to receive this newsletter, please send an email to training@iea.com.au with “unsubscribe newsletter” in the subject line, or click the link in the e-mail. Please note: you should unsubscribe using the same email address you used to subscribe with in order for this to take effect.

© IEA 2009. All rights reserved. You are free to use material from the Information Overload newsletter in whole or in part, as long as you include acknowledgement of source.

Information Enterprises Australia Pty Ltd
Unit 4, Upper Level, 201 High Street, FREMANTLE WA 6160
Tel: 08 9335 2533 Fax: 08 9335 2544 e-mail: training@iea.com.au