



# Information Overload

Issue 43, March 2006

---

## Welcome:

First of all we would like to say thank you to all those people who have registered for IEA's Inaugural Seminar on Electronic Document and Records Management Systems Seminar – EDRMS: Local People, Local Knowledge, we look forward to seeing you in June. For those of you who haven't yet booked your place, registrations are now open, and you can register online or download a copy of the registration brochure. Please visit – <http://www.iea.com.au> for more information.

The March edition of Information Overload takes another look at the safety of information, in particular electronic information. With the ever increasing number of pieces of malicious software (malware) doing the rounds, do you need to play host to unfriendly people (insiders) within your organisation so they can gain access to your information, or are there other more serious problems facing organisations today? As is the case with Information Overload we can only scratch the surface of this fascinating topic and we may not be able to offer solutions as to how to deal with the many problems faced by organisations every day, but we will give it a go.

We would like to thank you in advance for forwarding this onto friends, colleagues and other interested readers. Please note that all back issues of this edition, as well as our registrant resources edition can be read and/or downloaded from our web site – <http://www.iea.com.au> should any of the topics be of interest and use. For your information the March edition of the Registrant Resources edition looked at Advanced Internet Searching tips. If you have any suggestions or would like to see us cover any other topics, we would love to hear from you. Just send an e-mail to [training@iea.com.au](mailto:training@iea.com.au):

Lorraine Bradshaw  
Marketing & Training Coordinator

---

## In this Issue we will be looking at:

- An ethical dilemma
- Inside Information
- How sick is your system?
- Can we solve the problems?
- A Thought to ponder.

## An Ethical Dilemma

A couple of questions for you:

How many of you would deliberately go around the office where you worked and look through people's desk drawers looking for items you could "borrow"?

---

© IEA 2006. 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](mailto:training@iea.com.au)

Of those of you who did say they would "borrow" some of their colleagues' items, how many of you would return them?

Or consider this - How many of you have deliberately or accidentally sent (through electronic means) or taken sensitive information away from your organisation?

If I were to hazard a guess I would say that most people reading this, would draw the line at going through someone's personal belongings, because it was "wrong" but would not think twice about sending company information to the outside world, especially if working with collaborators on a project. But what has that got to do with "borrowing" from someone you work with? Actually we are not talking about the removal of "things" per se, but ideas. If you have ever taken credit for someone else's idea(s) or had your ideas used by someone else and they got the credit for it, then you will know what I mean.

Intellectual Property is a valuable commodity; it can sometimes mean the difference between a pay rise and promotion or not as the case may be, and whilst annoying to have someone else take the credit for your work, you can take steps to rectify the problems, or to ensure that it cannot happen again – lock your office door, "lock" your workstation, be careful who you tell, instigate a clear desk policy etc. However, on a company scale, the loss of Intellectual Property can literally make or break the organisation that you work for, especially when the information finds its way into the wrong kind of hands, deliberately or otherwise.

In today's working environment, most of the information relating to our organisations reside in an electronic format, and therein lies part of the problem. If you are sending information to a third party (internally or externally) how can you guarantee that the information that is sent will be used only for the purpose that it is intended? How can you guarantee that the information will be stored in a safe and secure location on the recipients email server? Can you guarantee that the person you are sending the information to is as honest in his/her dealings as you are? Or will you find your sensitive information in the hands of a competitor at some point down the track? It was interesting to note that "IDC estimates that 60% of business critical information is stored in messaging". *Gill, Christine, Bigger than Ben Hur, p54 Image and Data Manager September/October 2003* all of which can have a major impact on the way that your organisation operates.

One of the biggest problems with electronic information is that it can reside in more than one place at the same time. So how can you keep track of it, if you don't know where it is stored and how many copies there are? And as with all record keeping issues, how long do you need to keep it, where do you store it so you can find it again, and if you are going to destroy the item(s), how can you be sure that you have every copy of the document, given that most people will have stored a copy somewhere – just in case. And do you have any idea what is on your back up tapes? Is it any wonder that information goes missing and perhaps more worrying, finds its way into the wrong kind of people's hands (and computers).

Whilst electronic document management systems can help, it does not alleviate the problem entirely – especially if the system you are using is unwieldy and people don't understand the importance of keeping information in a secure location. The question is what can you do about it? However, before we answer that question, there are another couple of problems associated with the safety of intellectual property in an electronic world.

---

© IEA 2006. 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.

## Inside Information

The first scenario has nothing to do with everyone within your organisation having their own retention and disposal policy – my inbox is getting full, so I'll just get rid of a few messages!! Actually one of the more potentially damaging problems deals with “insiders”.

Insiders can be people who are deliberately planted to gain competitive advantage, or someone who takes advantage of inside information for personal gain. A report by the Financial Services Authority (FSA) in the UK found evidence “that organised crime groups are deliberately targeting firms by planting staff in the companies to commit commercial crime” *The Enemy Within, p34 Image and Data Manager July/August 2005*. And it's not just money that people are stealing, but the identities of the people who work for the organisation. Of course, along with the names, addresses and banking information, social security and other reference markers are needed to obtain items such as Credit Cards, Cheques, Drivers Licences and Passports.

The 2005 DOPIP (Document, Product and Intellectual Property) Security Council Intelligence Report, reported more than 291 incidents valued at US\$623,766,946 over 46 countries, with the USA being the biggest losers with an estimated \$87 Million. <http://newswire.com/pr38294.html> accessed 22.03.06

Believe it or not, music was not the number one item stolen. The most popular items were “Financial Instruments – with 118 incidents worth US\$509 Million”, with currency, cheques and credit cards all in the top ten of counterfeited items. (*op cit*).

In 2005 a study of 23 incidents in the U.S. financial sector was conducted by the U.S. Secret Service and Carnegie Mellon University found that most were not technically sophisticated or complex. 87% of the cases involved insiders using legitimate end user commands and 78% were authorised users with active computer accounts. Of these 81% were planned well in advance with other people being aware of what was going on, and it appears that these same insiders were only interested in the money, rather than deliberately harming the organisation. *The Enemy Within, p35 Image and Data Manager, July/August 2005*.

## How sick is your system?

However, there is another scenario that all organisations should be aware of, and that is - what happens when a third party intercepts your electronic communication, or worse still is lurking within your system capturing information as it is being generated. We are of course talking about viruses or perhaps more accurately – Trojans.

With the rapid spread of viruses, organisations may have a hard time keeping fire walls up to date, and whilst most people are getting wary by not opening mail that contains executable files (anything with a .exe attachment) they are still getting through and causing untold damage.

Keyloggers – designed to capture keyboard strokes and mouse clicks – useful if you want to capture password and account information.

However, one of the most interesting (if disturbing) trends has been the release of MyFip which seeks to find specific document extensions within an organisations system – predominantly .pdf. The reason it ran under the radar is that it was quietly capturing the data

---

© IEA 2006. 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.

and sending it back to the originators. What is disturbing is that a great deal of sensitive information is contained within reports, usually PDF documents that are distributed across organisations for discussion and may contain everything from the latest changes to systems security, through to product information, engineering drawings and everything else you can think of. So how did it get through? According to the LURQH Threat Intelligence Group, The website that links to the virus was offering exam material, and the MyFip virus was obviously designed to steal more sensitive data with the view to adding to its items for sale category, and has since added other extensions to its requirements list, including - .doc - Microsoft Word Document, .dwg - AutoCAD drawing, .sch - CirCAD schematic, .pcb - CirCAD circuit board layout, .dwt - AutoCAD template, .dwf - AutoCAD drawing, .max - ORCAD layout, .mdb - Microsoft Database. <http://www.lurhq.com/myfip.html>

So how do these things get through? Well as with most viruses we still need to execute the program contained in the message, and this is done by simply clicking the item open. A recent virus to do the rounds at IEA was nipped in the bud because we asked if the person reportedly sent an attachment through. As it turned out, the Director hadn't sent it, and we got rid of the problem, but what happens in large organisations when you can't ask those sorts of questions?

## Can we solve the problems?

Unfortunately the answer is "maybe". Whilst some of the problems can be countered with good security and email and internet policies, organisations dealing with electronic security always seem to be one step behind the virus writers. But for what it is worth the following are a few suggestions to make it harder to get a foot in the door.

- Don't open dodgy email attachments, even if they do come from the boss – if in doubt – ask first.
- Ensure your firewalls and virus protection are up to date.
- Have a policy to change passwords regularly and don't use dictionary type words, but don't make them so complicated that you can't remember them and have to write them down.
- If you work for a large organisation, make sure that you lock your workstation so that other people cannot go through your password protection to get to sensitive material.
- Encourage people to store documents in the correct location(s) so that the information can be captured and archived.
- Limit the use of personal drives – in an ideal world this would be one of the best ways to ensure that copies of documents are not scattered throughout the organisation. However, with a considerable amount of information being transacted through electronic mail, duplicates are still going to exist.
- Ensure that your organisation enforces their email policies, and whilst breaches can be hard to rectify once the sent button has been pressed (if you've ever tried to stuff toothpaste back into a tube you will know what I mean) you may be able to limit the damage done to your organisation.
- Ensure that you follow good practice in hiring the people who work for you. Do not accept photocopies of certificates as proof that a person says who they are and what they do are genuine. Good reference checking should help to weed out any potential problems.

- If you are about to “let people go” make sure the electronic access is cut. Passwords should be changed immediately and if your organisation deals with sensitive data, it might be a good idea to make sure they haven’t had time to send reams of information to an outside email account, or are planning on taking copies of documents on disc when they walk out of the door.

We hope you have a great week.

---

## **A Thought to Ponder:**

“The only way to get rid of temptation is to yield to it”

**Oscar Wilde**

1854-1900

---

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](mailto: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](mailto:training@iea.com.au) with “subscribe newsletter” in the subject line.

If you have any suggestions as to what should be included in future editions, then please send an email to [training@iea.com.au](mailto:training@iea.com.au). If you would prefer not to receive this newsletter, please send an email to [training@iea.com.au](mailto:training@iea.com.au) with “unsubscribe newsletter” in the subject line.

---

© IEA 2006. 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](mailto:training@iea.com.au)