



# Information Overload

Issue 37, September 2005

---

## Welcome:

Welcome to this month's edition of Information Overload. This month we ask a simple question – How safe is your data? With the recent devastation caused by Hurricanes, Cyclones and flooding – disaster planning and disaster management should be high on everyone's "to do" list. Do you know what vital records your organisation has; do you know where they are? And will you be able to access them should the unthinkable happen to your place of work. What about the safety of your electronic data? Is your system hacker proof, or do you have glaring holes in your security systems, practices and procedures? How good are your backup procedures – Do you have a backup procedure? As always we hope you enjoy reading.

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 Coordinator

---

## In this Issue we will be looking at:

- How safe is your data?
- Managing the problem; Determining the value of the data vs the cost of protection;
- Emails are records too;
- Media Fragility – Backups, Updates and Changes in Technology;
- Archival concerns;
- Accountability;
- Exit policies:
  - Making sure the "leavers" don't take the silver with them when they go!
  - Retirees, redundancies & those who die on the job.
- A Thought to ponder.

---

## How safe is your data?

A simple question perhaps, but one that can have many different answers, depending on what data you collect and ultimately what you end up doing with it. As you may already have realised, all data is not created equal. It is the building blocks or foundation on which "information" is used, knowledge is gained and decisions made. But without some sort of analysis, "data" on its own is just stuff we generate and collect. As we go about our personal lives and daily tasks, we all collect "data", more often than not, we sift what comes

---

© IEA 2005. 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)

in to our collective memory, file away what is useful, use what we need to use now, and discard the rest in a mental “dumpster”. Data collection and analysis for most people is instinctive, we simply don’t think about it.

However, when it comes to a larger collective of people, groups, partnerships, businesses, organisations, even a group of friends, we all collect data, we analyse what we personally collect and sometimes we disseminate what we find to the other members of the collective, but sometimes we don’t – after all “knowledge is power” and some people like to “hoard” what they find and what they know. One of the biggest problems I find with the dissemination of information is that we only disseminate what we think the other people may want, rather than what they may need.

As we share, our collective memory banks grow and it can be said therefore, so does our knowledge, and the collective knowledge of the organisation or group to which we belong. Knowledge is the body of understanding and skills that is mentally constructed by people using the data that has been collected, analysis performed to turn data into information, and collectively used to become knowledge. It is said that knowledge can only grow when it is shared – usually with other people.

Knowledge management, it can be argued is not about the management of “knowledge” per se, but the management of the data that may or may not become knowledge, depending upon the analyses that are performed upon it. The question is, how do we manage it?

### **Managing the problem: Determining the value of the data vs the cost of protection**

If not all data is created equal, should it be treated in the same way? The answer as we have mentioned before comes down to a couple of points. It depends what the data is, why it is being collected, and what are the legal considerations for not managing it.

As with most things electronic, there is no silver bullet. What seems to work for one organisation will probably not work in another, even if the organisations are similar in size and nature. The reasons are varied, but can be as simple as the fact that organisation A wants the system, and wants it to work, so therefore they will do whatever it is that needs to be done in order to make it work. Organisation B on the other hand, have been told that it’s a good idea, and they must follow the rules, or else. So they try it for a while, but as they thought, it just isn’t going to work for them – because. There is not a one size fits all policy when it comes to managing data. The systems and the solutions must be scaleable, and they must be able to “grow” as the size of the problem grows, and as the organisation grows and changes.

### **E mails are records too:**

The system you choose must be flexible in that it must be able to manage all types of data, including e-mails, SMS messages, Voice over Internet (VOIP) and MSN messages, especially as emails have been used as evidence in many court cases, including the United Kingdom's "Hutton Inquiry", and those emails sent and received by journalist Andrew Gilligan. The Hutton Inquiry was a British judicial inquiry chaired by Lord Hutton who was appointed by the British government to investigate the death of a government weapons expert, Dr. David Kelly. As a result of the inquiry, changes to British Legislation occurred. The Retention of Communications Data Under Part 11: Anti-Terrorism, Crime & Security Act 2001 - <http://www.hms.gov.uk/si/si2003/draft/5b.pdf> now stipulates that information relating to email traffic should be retained for a period of 12 months. In fact any record “which is sent and received as part of a business transaction should be subject to the same retention and disposal schedules as the rest of the electronic and paper based records managed by an organisation”. *Section 1: What is a Record? Australian Record Retention Manual, 5<sup>th</sup> Edition, 2004*

Electronic messages and in particular emails that have been sent and received by individuals within certain organisations have been found and presented as evidence in a court of law, despite being "deleted" from the system – for example *UBS Warburg - 2004*. Whilst other organisations have been fined considerable amounts of money for failing to provide e-mails, and failing to preserve emails and other documents after being told they were under investigation. Banc of America securities was fined US\$10 million, Philip Morris and the Altria Group were fined US\$2.75 million. *Computerworld June 15 2005, p24-25 Record Risks*. It is still interesting to note that according to a survey conducted by the Association of Records Managers and Administrators (ARMA) and the Association of Information and Image Management (AIIM) 65% of organisations still do not have an e-records policy, nor the technology in which to ensure that it can comply. *Computerworld June 15 2005, p24-25 Record Risks*

An effective email policy should encompass - what you should and should not say, do, print, save and where to store it once a decision has been made. Easier said than done of course, but it can be the difference between being fined, jailed, dismissed or not. It may also prevent your organisation being the target of viruses, trojans, worms, being used as a relay station for sending out spam and subsequent black listing if you are accused – but that depends on the quality of your firewall, the ease in which hackers can penetrate your system and appropriate the data, how often you insist your employees change their passwords, whether or not those passwords are dictionary based and therefore "guessable" by password cracking software, whether or not the software patches on your system is up to date, and who has access to your machine when you are not in the office. Why bother to install all the latest firewalls and security devices if you do not vet your employees! As we mentioned in the last edition of Information Overload – organisations are now being targeted from the inside. Why bother hacking into a system, when you can work directly for the organisation and obtain the information using legitimate commands and account information.

### **Media Fragility – Backups, Updates and Changes in Technology**

We seem to have a very short memory when it comes to computer technology, we know that the operating system that we are running today will be replaced with a more modern equivalent in the not too distant future. We also know that it will be installed with little thought or regard as to how much data we will lose as a direct result of the upgrade. Does anyone remember trying to upgrade through the early versions of windows? And if you waited too long between upgrades then chances were good that you couldn't read the old data, let alone migrate it. Technological obsolescence is still a major problem for all organisations. Despite many projects, thousands of dollars and hundreds of person hours, we are still wading through the problem of trying to keep pace with the changes in technology, and access to our material.

So what can we do to ensure that we can still read the data when we need to?

Migration is important. Keeping your data "live" can ensure that all material can be read, assuming you still run the software that it was created on of course. In keeping material "live" you should also ensure that you save a copy – just in case. Regular backups can help with several key problem areas, including technology and building failure, through natural disasters and terrorist activities. Ensuring your data is backed up can and does play an important role in disaster planning, and organisations should ensure that all key data is backed up to another media at least once a day, more if your organisation deems necessary. Being able to access those same backup tapes (or other media used for the purpose) can sometimes be the difference between survival or not for the company. It has been said that:

- 70% of organisations that suffer paperwork and computer loss go under within 3 years (McDougall, 1989)
- 43% of businesses never re-open and a further 29% go under within 12 months. (Datapro Research, 1990)
- 50% never recover from a major incident. (Sarkus, 1992)
- There is only a 10% survival rate after a major computer crash. (White, 1989)
- 48% of organisations cannot tolerate more than 24 hours of downtime (KPMG, 2002)

Determining what data is classed as mission critical will vary from organisation to organisation, whilst some vital records may be similar to the organisation next door, only you can determine what you will need in order to get back up and running. Can you afford any "down time"? Can you recover all of your lost data, or only some of it?

If your system cannot be down for any period of time, then perhaps another option would be to house mirror information off site, and away from the seat of the main operations. However, with the large-scale disasters that have been happening of late – how far is far enough away?

### **Archival concerns**

However, there will come a time when the material you have stored does not need to be accessed on a daily basis. For example, employees who no longer work for you, or there is a project you are no longer working on. This information is still important and needs to be retained, just not accessed on a daily basis. Employee information for instance needs to be kept until the person reaches 71 years of age. Information relating to a structure that your organisation designed and built needs to be kept for the life of the building. If this information is stored electronically you need to ensure that your systems can handle that information now and well into the future. Therefore it needs to be protected, not only from accidental or deliberate deletion or mishandling, but you will also need to ensure that your technology can withstand hackers, bugs and other electronic vermin. Migration through media may be the answer, although a thorough check to ensure data is not lost as part of the conversion process is essential. If the data is not stored in a live environment then it should undergo a periodic but regular "refresh" process. This is the process whereby the data is copied from one form of media to a newer version of the same media eg., tape to tape. This is important because there is currently no way of determining how long data stored in an electronic format can last. Whilst there are some claims made by the manufacturers of the media that the technology has a certain lifespan, the technology has not been around long enough to test the validity of the statements, and it appears that the technology is unlikely to remain the same long enough in order to test the statement.

A recent news report has indicated that there will be a DVD format war as the backers of one standard said today that there is no common ground for a unified format and that it is on track for a market launch within a year.

[http://www.computerworld.com/hardwaretopics/storage/story/0,10801,104341,00.html?source=NLT\\_AM&nid=104341](http://www.computerworld.com/hardwaretopics/storage/story/0,10801,104341,00.html?source=NLT_AM&nid=104341)

DVD has been the fastest-adopted technology in consumer electronics history and has generated billions of dollars in royalties for the inventors, a broad base of consumer electronics companies including firms now divided over its successor. The fight for license income may yet hurt the interests of consumers, who face two disk formats that do not play back in all devices, invoking memories of the VHS-Betamax war for the VHS standard, or

---

© IEA 2005. 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.

more recently, the rewritable DVD standard. *DVD format war looms as Blu-ray backers plan launch. News Story by Lucas van Grinsven. September 02, 2005 (Reuters).*

### **Accountability:**

But who's problem is it? The individual, the IT department, the Organisation, the manufacturers of the media and/or technology or the Records Manager?

There should be an element of accountability for all when it comes to managing documents, records and the data from which these were formed.

The system(s) should be easy and simple to use, otherwise people will find all sorts of reasons to keep items out of the system. But is it up to the individual to ensure that they do something with the records they create? Should the organisation manage the problem centrally? Does anyone remember the time before computers? When secretarial pools were the norm, and only 5 copies of a document could be typed at any one time, using carbon paper between each copy if you wanted to ensure each copy was still readable. Each copy had a designated purpose and someone managed it. With the increasing use of computers, everyone and anyone can receive a copy of every document an organisation produces, and can do so anonymously which makes managing them a major problem. A good records management policy can go some way towards solving some of the problems as can having an effective retention and disposal schedule. But in most cases, it relies on systems being in place to handle the large volumes of traffic a modern organisation generates, along with a considerable amount of goodwill from every member of staff.

What it does not seem to handle effectively are those records kept by people "just in case" they need something later on. Copies stored on hard drives, and backup tapes that are impossible to get rid of because some of the information contained on the medium needs to be kept forever, and finding that single incriminating piece of evidence that started life as an email is stuck in the middle of it. And of course the fines that are associated with the failure to keep the correct records for the correct length of time and in a format that is acceptable in a court of law, is also considerable. The new edition of the Australian Record Retention Manual (ARRM) will see almost 2,000 individual pieces of legislation associated with the keeping of records. Of course not every piece of legislation contained in the manual will affect every organisation, but knowing what does affect your organisation can be an interesting challenge. For more information on the ARRM please visit our web site – <http://www.iea.com.au>.

Another area to be considered is that of version control – the problems associated with managing electronic information are interesting as they are varied. Documents can be re-written and over-written, saved as an entirely different document and moved into another area of the system as fast as a click of a mouse button. There are no furtive trips needed to find the document and a photocopier that isn't being used in order to make a copy of the document in today's electronic environment. There are a couple of questions that need to be asked when looking at any document:

- Is the version I am viewing the version that the originator wanted me to see?
- Is it in the correct format?
- Can I see the object in the same way as the original creator saw it?
- And does it matter?

Do you really need a million dollar solution to a thousand dollar problem? According to Wade Dewald, a senior vice president of Sogeti, an American computer consulting company "ninety five percent of e-mails are not worth saving for long. Only 5% are truly records." Jim Pollock of the Des Moines Business Record – Central Iowa's Weekly Business Journal wrote

---

© IEA 2005. 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.

on Sunday, September 4 2005, that "Morgan Stanley, the financial services giant should be fined \$10 million for failing to hold on to e-mails that the SEC wants to see as part of an investigation. Three years ago, Morgan Stanley was fined \$1.65 million for its poor record-keeping." <http://www.businessrecord.com> - *Lawsuits spur companies' interests in e-mail archiving*. As with most things it usually takes some sort of precedent to occur before others begin to take notice. But the mentality of "it won't happen here" is still evident, with organisations shrugging their collective shoulders, would it be cheaper to pay the fine(s) rather than manage the problem?

### **Exit policies:**

#### **Making sure the "leavers" don't take the silver with them when they go!**

Do you have an exit policy for those people who are leaving the place where you work? Whilst some of this should be covered by the HR department, for example keys, credit cards, passes, it should be part of each departments role and responsibilities to ensure that the "leavers" only take with them what they should and not what they want. Do you have a policy to ensure that all reports and files are returned to the records department before they leave? Are all library books returned? Is a check made of all emails being sent "home" on the person's last day that may contain confidential and/or mission critical information? For those people who are being "asked to leave" this is the time to ensure that all email and internet access is denied. Of course this does not stop people taking information with them. Someone who has known that they were going to be leaving for some time will have made certain arrangements before the last day.

Take for example research and development organisations such as pharmaceutical companies – it appears to be standard policy for all "leavers" to be accompanied whilst they clear out their desks, in some cases, desk clearing is done by a senior staff member and security personnel, and then the person is escorted to their cars to ensure they do not take anything with them when they leave. Dramatic? Not when you consider that industrial espionage is big business, head hunting is rife, and the time it can take to get a drug to market is measured in years and millions of dollars. The individual knowledge held by each employee can be given and/or sold to the next organisation they work for. Whilst confidentiality agreements may be signed, and enforceable – ie., you cannot work for a competitor for a period of time, how many of you have inadvertently let slip information on an organisation you used to work for?

### **Retirees, redundancies & those who die on the job.**

Before you think I am being completely morbid. I have known several instances where key personnel literally died at their desks, taking with them countless years of experience and knowledge with them when they went. And because these people "went suddenly" there was no way of handing over the reigns to someone else, there just wasn't time. Whilst retirees and those people who are being made redundant can pass on some of the knowledge they had gained during their tenure, it is a little harder to plan for people dying. What would you do if one or more of your key players suddenly weren't there? Would your organisation be able to survive? In the aftermath of September 11, it was revealed that a number of organisations lost more than one key player. Bond-trading firm Cantor Fitzgerald lost about 700 of its 1,000 World Trade Center workers, including many top executives. And Jimmy Dunne a principal executive at investment banking firm Sandler O'Neill & Partners expressed how overwhelming it is to face a future without a company's established leadership. Mr Dunne, was away from the office when the World Trade Center was attacked, however chief executive Herman Sandler and investment banking chief Christopher Quackenbush died in the building's collapse. Dunne suddenly found himself in

---

© IEA 2005. 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.

charge. The problem was that he alone could not duplicate the strengths that each partner had brought to the firm. As reported in <http://www.workforce.com/section/00/feature/22/97/54/>

Whilst this is quite a dramatic example of what can happen when disaster strikes an organisation, recent examples of hurricanes, cyclones and earthquakes and the aftermath of each event can show how tenuous a hold we each have on society. Succession planning, job sharing and rotation, good records management policies and a disaster plan are just some of the suggestions we can utilize to ensure our knowledge isn't lost.

We hope this has given you some food for thought, if you have any questions, or would like to speak to any of the team at Information Enterprises Australia with regards to managing your data, please contact us on 08 9335 2533 or email [consulting@iea.com.au](mailto:consulting@iea.com.au).

We look forward to speaking with you.

---

## A Thought to Ponder:

**"Knowledge might be power, but only when you take action."**

Richard Keeves

---

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 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. 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).

---

© IEA 2005. 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)