



Information Overload

Issue 29, January 2005

Welcome:

Welcome to this month's edition of Information Overload. With the recent global disasters that have affected so many people across the world, the bush fires raging across Australia, and people being evacuated from their homes it is perhaps an appropriate time to ask the question. Do you know what you would take with you, if you only had a few minutes to get out of your house? What would you leave behind? Would you take pictures and photographs, your computer? Or the tools of your trade? What about family heirlooms, clothes and special toys for the kids? What about people and pets? For those people who have dogs and cats its relatively easy to scoop them up and put them into the car, but what about those people who have birds and livestock such as horses and chickens? Do you leave them to their fate and hope they are still there when you are allowed back to your property? Or do you set them free and hope they don't get in the way of the rescue effort? This month we take a look at disaster planning and suggestions for putting together a disaster plan for your organisation.

As always, 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.

We hope you enjoy reading.

Lorraine Bradshaw
Marketing & Training Coordinator

In this Issue we will be looking at:

- Disastrous
- Types of Disasters
- Determining your risk
- Creating a Disaster Plan for your Organisation
- A Thought to Ponder.

Disastrous

Terrorism, tsunamis, bush fires, earthquakes and volcanic eruptions, one can almost be forgiven for thinking that we'll have plagues of flies, frogs and locusts next. We have seen some of the worst natural disasters in recent times and with the added impact of civil war across many countries, genocide and the ongoing threat of terrorism I have to marvel at the capacity of "man's" ability to cope with whatever is thrown at us.

We do not choose the type, the time or the severity of disasters. They are by their very definition a "sudden or great misfortune" or simply "any unfortunate event whose timing is unexpected and whose consequences are seriously destructive". www.system.missouri.edu/records/dpa1.html

Your response and that of your organisation is critical and you will be under considerable pressure to make sure that your response is the best one under the circumstances.

Speaking with a senior member of the WA Red Cross shortly after the Asian Tsunami, it became very clear that the loss of life, the number of countries affected and the scale of the relief effort needed, would re-write the parameters and boundaries of what a disaster is and its impact on the global population. It was said on more than one occasion we "now have a new and terrifying benchmark to measure future disasters against."

© 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

Disaster planning sounds like something of a misnomer. We may never see destruction on the same scale again, the question is how on earth do you plan for something that may never happen? It has been said that disaster planning is like having insurance. You decide on the level of cover that you want and then hope that you never have to use it.

Types of Disaster:

In addition to the natural events, acts of terrorism and war that we have mentioned, disasters can also include:

- Building failure – malfunctioning sprinklers, heating or air conditioning, leaks, faulty wiring
- Industrial accidents – nuclear and/or chemical spills
- Technology – system crashes, viruses, hard drive failures, back up tape drive failures
- Criminal behaviour – hacking, theft, arson, espionage, vandalism, riots, terrorism & war
- Accidental loss through human error

If we take the simple example of a hard drive failure, to some people this is just a minor inconvenience. Yes you might have lost a few personal items that were housed on your hard drive, but everything else is still on the server. Plug in a new computer, load up the software and you can be back up and working in a short space of time. However, to some people without the benefit of a server to backup to every night, the loss of a computer hard drive is disastrous. How many people ensure that they have backed up every item on their home computer? I know that some of my personal documents and writing are backed onto disc, some are even backed up to the internet, but not all of them. Re-creating the items that I could potentially lose? Almost impossible! So why am I not more concerned with this potential disaster? Well I must admit that it has something to do with the mentality “it can’t happen to me!”

Can it happen to you?

It is said that every organization will face some sort of disaster during its operational lifetime; the test is how quickly you can recover. It is 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)

It happened to these organisations:

1988 – Floods at the Supreme Court of WA

1994 – Fire in the Architectural Division of the West Australian Building Management Authority

1994 – Fire in the Fremantle Law Courts

2002 – City of Subiaco lost their roof during a storm, the staff had to work quickly to dry rain soaked paper to prevent mould growth.

Determining your risk

Some organisations are more susceptible to disasters than others. For example, research companies, pharmaceutical and chemical companies, abortion clinics are at risk not only from explosions, chemical contaminants but industrial espionage and persons opposed to what you do. In determining your risk you need to look at the type of work that you engage in, where your building is located, is there a history of “disasters” in the area or even within your organisation, can lightning strike twice in the same place? and whether or not you have a good records management system in place should

© 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.

the unthinkable happen and you have to recreate your organisation from the records that you can find or get access to.

One of the most important ways you can identify potential disasters is to conduct regular risk audits of the building and its surroundings, and records storage locations. A risk audit involves examining the following to detect risks:

- Building location(s): - are they close to rivers? airports? chemical factories? industrial zones?
- Building Structure and fabric: - for example, wire and pipe positioning and state of repair
- Existing fire and water detection systems
- Existing fire suppression systems
- Existing maintenance regimes: for example, cleaning, servicing of heating ventilation and air conditioning systems, and electricity

Storage Areas –

- Electronic recordkeeping systems – Security, passwords, backups, offsite storage
- Security control measures – appointments (are people escorted to and from the building), inductions, dismissals, audit logs of access (computer and visitors)
- Relevant procedures - for example, smoking restrictions and records handling procedures

Creating a Disaster Plan for your Organisation

Creating a disaster plan should have the backing and support from the entire organisation and should have input from each business unit, including the Library, Archives, Records Management and Information Systems teams.

The plan should contain:

- Emergency Information Sheet - one page summary of immediate steps to be taken and individuals to be contacted.
- Introduction to the plan - purpose, author, organisation and scheduled updates. The plan should be reviewed regularly and should take into account systems changes and upgrades and any changes to personnel and personal information including telephone numbers.
- Communication Plan - (telephone tree) – include names, numbers, methods, alternatives – eg., next of kin and chain of command – who to contact first etc – include – police and emergency services if you are the first person to notice the problem
- Procedures for identification and declaration of disaster situation and initiation of the disaster response chain of command
- Collection Priorities - locations and name/address of collection specialists eg., IT
- List of vital records – in a general sense a vital record is one, which proves ownership of property, equipment, vehicles and products and should include, contracts agreements and insurance documents, as well as financial data and personnel records. Without these records it is unlikely that a business will be able to resume operations and will ultimately cause the business to fail.
- Provisions for training of team(s)
- Checklist of pre-disaster actions - when disasters can have advance warning – eg., hurricanes and floods – assign duties and backups
- Instructions for response and recovery - Summary of steps for the recovery and salvage of material. When determining the risk associated with your organisation it is useful to summarise the procedures/steps for each “likely” occurrence.

© 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.

Should also include:

- Recovery team members
- List of sources of back up resources, include expertise, tradespeople, materials, equipments, vehicles and accommodation. For example - Where to get spare computers, setting up an alternative office, organizing the recovery of back up tapes from secure offsite storage and re-loading – depending on how often you backup and to where will determine how much critical day-to-day and other records have been lost – If the “disaster” occurs during office hours and routine back up does not occur until the evening/over night, the loss could be significant.
- Rehabilitation – Procedures for activities including marking and labeling, rebinding and repair, re-housing manuscript/archival material, sorting and re-housing, smoke/soot removal, cleaning etc.
- Multiple copies of record keeping forms, including inventory, packing lists etc
- Plans - covering all aspects including exits, windows, fire extinguishers and alarms, sprinklers, smoke detectors, water, gas, priority collections
- Accounting info – funds available for recovery effort and procedures/authorisation for access.
- Insurance info – coverage, claim procedures, record keeping requirements, state/federal disaster relief procedures.
- Keys - Location and access to, combinations for special collections, elevators, (may just be a requirement to have the person(s) responsible for the keys/collections etc listed for security reasons).

A Thought to Ponder:

“When I hear somebody sigh, 'Life is hard,' I am always tempted to ask, 'Compared to what?’”

Sydney Harris

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 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. If you have any suggestions as to what should be included in future editions, then please send an email to 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