Jeff Murray

Director Knowledge and IT Service Centre, Edith Cowan University

A newfies guide to risk management

Risk management is the sum of all activities directed toward acceptably accommodating the possibility of a failure in a program. The modern librarian faces daily challenges in managing, avoiding and ameliorating risk. Events like the Y2K problem (year 2000, now a past and fading memory) and the tragic events of 11 September 2001 have spurred a growing interest in ameliorating and preventing the impact of regular and common business risks, as well as those associated with disaster.

Risk management has been used to highlight the need to move the defensive line to a much earlier stage. 'Prevention is better than cure' is a common catch-cry of auditors and risk managers, and risk management involves the systematic identification of and planning for the avoidance or recovery from incurred risk.

Why bother?

It's a frightening statistic – in a 40-year professional career a librarian has 2 chances in 5 of participating in a major disaster recovery at work. The 2003 CAVAL survey of 18 Australian university libraries found that 27 per cent of the respondents had faced a significant disaster/emergency in the preceding six years. It is important to bother with risk management because there is a real chance that at least once in the next decade you will have to recover from something that has disrupted your service.

What to do

Risk management involves the systematic identification of the likelihood and impact of a disruption occurring. In 2003, 83 per cent of Australian university libraries had a disaster recovery plan and the chances are the statistics are similar for other sectors. However, these plans are often not complete, do not contain sufficient detail or cover relevant areas, or are not supported through testing or training.

Get involved and contribute! National Advisory Congress 2006, 19 September 2006

The national meeting will be held in association with the CLICK 06 conference – a half-day national meeting from 1:00pm–4:00pm on 19 September 2006.

The following regional meetings will be held mid-July to late-August prior to the national meeting:

- NSW: Sydney, contact: Niki Kallenburger, niki.kallengerger@alia.org.au; and Northern Rivers - Claudia Davies, claudia.davies@alia.org.au.
- QLD: Brisbane and Mackay, contact: Claudia Davies, claudia.davies@alia.org.au.
- NT: Darwin, contact: Sue Chilman; and Alice Springs, contact: Nathalie Smith.
- WA: Perth, contact: to be confirmed.
- SA: Adelaide, contact: Fiona Butcher, fiona.butcher@alia.org.au.
- VIC: Melbourne and Ballarat, contact: Margie Anderson, margie.anderson@alia.org.au.
- TAS: Hobart and Launceston, contact: Jane Jeppson, jane.jeppson@alia.org.au.
- ACT: Canberra, contact: Georgina Dale, georgina.dale@alia.org.au.

For additional information on the ALIA 2006 National Advisory congress please see: http://alia.org.au/governance/nac/.

- Only 77 per cent of plans contained salvage techniques.
- As few as 38 per cent covered business continuity.
- Only half covered technological risk.
- Just over half (55 per cent) trained staff in preventive risk management.

An effective risk management strategy involves not only identifying the likelihood and impact of potential risks, but also documents qualitative measures of the consequence or impact of the risk. Impacts might include:

- injury (perhaps from falling equipment and furniture, or even aggressive patrons;
- financial or asset loss (potentially from damaged collection items);
- interruption to service (from unauthorised and damaging hackers accessing the electronic catalogue database)
- reputation and image damage from the publicity associated with a disaster
- poor performance outcomes (from possibly higher than expected costs due to sudden changes in international exchange rates)

The next step in proactive risk alleviation involves planning to mitigate or prevent the risk happening in the first place. For those unavoidable risks, like natural disasters, a treatment plan is put in place. There are many ways to manage risk.

- Avoid and reduce the risk: for example, collection shrinkage is lowered by security gates and magnetic strips placed in books (reduction strategies).
- *Substitute* the risk, including strategies like installing fire sprinklers to reduce the risk of fire, and replace it with the risk of water damage
- *Engineer* the risk out by installing firewalls, demilitarized server zones on your network, having failover servers to maintain service continuity.
- Improve procedures and controls: regularly monitor the collections acquittals against the annual budget to ensure overspending does not occur.
- *Transfer* the risk by insuring the collection and valuable items.
- *Plan for recovery* by developing a business continuity plan and/or disaster recovery plan.

All too often this last point is left to the IT Department as they have learned from their Year 2000 experiences. However, many business units are missing a valuable opportunity to keep their service afloat even during disruptions for the simple reason that they simply haven't put alternatives in place. For example, some managers complain about computer outages (and rightly so) and yet they may not have an alternative source of information in place and are not well prepared for extended power failures or loss of their computers for other reasons. A risk management plan might also include evidence that the collection insurance cover has been checked for currency and relevance. Some state government organisations choose to be self-insurers and have contingency funds available to cover large loss items. These provisions need to be checked, not only for what is covered but specifically for what occurrences. Flood damage, for example, can be an occurrence that is strictly interpreted to cover natural disasters (like flooding from storms) but not pipe breakages and accidental fire sprinkler damage (that may have occurred through negligence).

If a disaster happens

A disaster is any incident that threatens human safety and or damages, or threatens to damage, a library's buildings, collections (or item(s) therein), equipment and systems. A disaster can be manmade or natural.

The disaster recovery discipline is a subset of risk management. The risk of a disaster has to be controlled and informed. And the process to do this is very similar to that identified above in the discussion on risk management.

In relation to disaster management, there are four steps to mitigating risk: these are to identify, analyse, evaluate and treat. Perhaps a single most important difference between disaster recovery and risk management is the higher importance placed on testing the disaster recovery plan. Annual or more frequent exercises are needed, involving mock disasters and staff responding by practising drills (such as removing valuable portable items from the building).

External help from risk management experts is probably a good idea. These external experts will vary depending on the type of risk under evaluation. For example most fire safety planning is designed to reduce injury and death, so a representative of the Fire Department will assist in this regard although he or she may not be too concerned about the protection of property within the building. Other consultants, possibly in risk planning, will deal with this area. Personal safety and protection of property are strong risk possibilities and must be balanced against one another in the event the worst happens and a fire breaks out.

The important elements of a disaster control plan will

- identify who is responsible for disaster management.
- contain catalogues and inventories as essential recovery documents.
- detail how the plan will be tested, including staff training measures.
- involve and annual, or more frequent, reviews of the plan.

Where can you get help?

A few simple resources of interest to anyone thinking about risk management.

http://www.rmia.org.au

http://www.riskman.unsw.edu.au

http://www.ecu.edu.au/RMAA/index.html

- http://www.riskmanagement.com.au (includes the third edition of the Standards Australia standard on Risk Management AS/NZA 4360:2004)
- http://www.caul.ecu.edu.au (includes the CAVAL Disaster Response Plans Survey)
- http://www.ecu.edu.au/RMAA/rm/rm_beginners.html Draber, P; Brennan, T and Wilson, A. 'Risk management for beginners'.

References

- Beamsley, T G (1999). 'Securing digital image assets in museums and libraries: A risk management approach', *Library Trends*, Fall 1999, 48(2):359–78. http://www.findarticles.com/p/articles/mi_m1387/ is_2_48/ai_59473805
- Eden, P and Matthews, G (1997). 'Disaster management in libraries', *Facilities*, Jan/Feb 1997, 15(1/2):42–49.

Linking people with ideas...



Australian

Library and Information

Association

ALIA's premier awards

Nominations are now being called for the following premier awards of the Australian Library and Information Association

HCL Anderson Award

The HCL Anderson Award is the Association's highest honour that can be bestowed on an Associate member of ALIA. It is awarded in recognition of outstanding service to the library and information profession in Australia, to ALIA, or to the theory of library and information science or to the practice of library and information services.

Applicants are required to be financial members of ALIA. This award is peer-nominated.

Redmond Barry Award

The Redmond Barry Award is the Association's highest honour that can be bestowed on an individual not eligible for associate or technician membership of the Association." It is awarded in recognition of outstanding service to or promotion of a library and information service or libraries and information services, or to the theory or practice of library and information science, or an associated field.

Nominees do not need to be a member of the Association. This award is peer-nominated.

Ellinor Archer Pioneer Award

The Ellinor Archer Pioneer Award recognises pioneering work in new areas of library and information science. This may involve a one-off product, a new service or program or development of an existing service, but must incorporate a future-oriented approach.

Applicants are required to be financial members of ALIA.

The nomination may identify a specific group or unit within an institution. This award is peer-nominated.

Nomination forms

Nomination forms and further information: http://alia.org.au/awards/ ALIA National Office, PO Box 6335, Kingston 2604 <u>awards@ali</u>a.org.au 02 6215 8235

Nominations close 1 August 2006

July 2006

