

The graphic features the letters 'IT' in a large, white, distressed font at the top. Below them, the words 'DISASTER RECOVERY' are written in a clean, white, sans-serif font. The background is a dark blue, textured surface resembling shattered glass or ice, with light reflecting off the sharp edges of the fragments.

IT DISASTER RECOVERY

The value of disaster recovery planning has been repeatedly demonstrated in Australia over the last few years. Flood and fire have taught us well and the whole world looked to Queensland's innovative library professionals who were able to protect unique resources in recent floods. But Greg Wyman, Vice-President Asia Pacific of StorageCraft says it is still true that there are two sorts of IT system users in the world – those who have lost data and those who will lose data. Planning, and knowing what's now possible is what will make the difference.

Ask anyone working in computer technology what their worst nightmare is and almost all will reply: 'server crash'. Servers are the computers that drive a library's network. They may not be in view on the front desk but they are the beating heart of just about everything the library does, and when they crash it can take hours or even days to repair or replace them.

Technical staff need to re-install operating systems (with a best case scenario of two to six hours), as well as all the applications, service packs, security updates, patches and more. Next comes the tricky part – trying to restore data from last night's backup (provided the backup worked correctly). And the whole time a server is down, library staff remains unproductive.

Imagine trying to run an up-to-the-minute information service without email or internet, and with no access to files. Inventory, customer databases, calendars, borrowing history - even security services and scanners would all be impacted.

Yet with a few simple steps and a little forward planning, it is easy to provide peace of mind, assure continuity of workflow to staff and customers and protect those vital data files. Fortunately technology has advanced recently, making it quicker, cheaper and much faster to protect digital assets.

From your information technology manager's point of view, the fundamental goal of any disaster recovery (DR) plan is to minimise data loss and downtime. While no single plan covers all businesses and facilities, some fundamentals simply must be included. Prevention is the first priority, followed by early detection, then correction of the problem.

Disaster recovery plans are measured by recovery time objectives (RTO) and recovery point objectives (RPO). Essentially, this means the length of time it takes to get a library's services up and running after a crash and the point at which data is saved, because the system can be restarted from that point.