Business Continuity Planning: Information Technology Aspect

INTRODUCTION

With the demise the large, expensive, mainframe computer housed in a computer center and run in a self-contained environment it might be thought that disaster recovery would be less of an issue. Online, real-time, networked, server-driven applications have become commonplace in all business environments, including CGIAR centers. However, because computer systems and business/research activities are often interdependent, computer applications are no less essential to business continuity. In fact, the very nature of user-interactive, online systems significantly complicates a recovery strategy. Many mission-critical applications currently reside on PCs or user-controlled application servers that are completely under the control of end users. Thus the ability to process end-user or research project applications in the event of a disaster may be crucial to a CGIAR center.

GOOD PRACTICE

Successful business continuity plans must be complete, current, and well documented. Specifically, the plan should describe the role of senior management; the recovery teams' responsibilities; plan testing; recovery alternatives; critical operational procedures; and other emergency information that persons may not remember in the middle of a disaster. The aim is to minimize the need for critical decision making in a crisis situation. As with any business program, the business continuity plan must be operationally feasible. The business impact analysis (BIA) is the foundation of effective disaster recovery planning. It must originate from the individual business/research areas and should highlight inherent risks and critical threats to achieving business/research goals. An IT unit is not self-serving; it is there to support the goals of the CGIAR center, whether they are business or research oriented. The more the business continuity plan is defined in relation to the center's mission, the easier it will be to sell to senior management and secure adequate funding for its implementation. The business continuity plan must be tested. Most IT staffs are committed and will perform beyond their normal expectancies in times of...
crisis, but if the plan has not been tested, there is a better than average chance that some of the procedures will not work. It is better for the plan's shortcomings to be revealed during a test than in a full blown crisis. Several levels of test can be employed:

- Hypothetical (dry run of plan processes): This is the cheapest alternative but may not expose all the deficiencies in a plan. However, it can expose obvious oversights.
- Component or multiple components: Various disaster scenarios can be explored and the plan tested against partial disasters.
- Module or several modules together.
- A full test.

It is important that a full debrief take place after each test and the plan modified where required.

The COBIT (Control Objectives for Information and Related Technology) framework was released in 1996 and updated in 1998 and 2000 by the Information Systems Audit and Control Foundation in response to the need for a reference framework for security and control in IT. COBIT guidelines can be considered best practice in any area of IT security and control, including IT business continuity planning.

Key considerations, according to COBIT, when considering business continuity planning are:

- Organizational policies require a disaster recovery/contingency framework and be part of normal operational requirements for both the information services function and all organizations dependent on information systems resources;
- IT disaster recovery/contingency planning requires:
  - a consistent philosophy and framework relating to development of disaster recovery/contingency plan development;
  - a prioritization of applications with respect to timeliness of recovery and return;
  - risk assessment and insurance consideration for loss of business in disaster recovery/contingency situations for information services function as well as users of resources;
  - an outline of the specific roles and responsibilities with respect to disaster recovery/contingency planning with specific test, maintenance, and update requirements;
  - information on formal contract arrangements with vendors to provide services in event of disaster, including back up site facility or relationship, in advance of actual need; and
  - minimum content to include:
    - emergency procedures to ensure the safety of all affected staff members;
    - roles and responsibilities of information's systems services function, vendors providing disaster recovery services, users of services, and support administrative personnel;
• a disaster recovery framework consistent with long-range contingency plans;
• listing of systems resources requiring alternatives (hardware, peripherals, software);
• listing of highest to lowest priority applications, required recovery times, and expected performance norms;
• administrative functions for communicating and providing support services such as benefits, payroll, external communications, cost tracking, etc in event of disaster;
• various disaster scenarios from minor to loss of total capability and response to each in sufficient detail for step-by-step execution;
• specific equipment and supply needs that are identified such as high speed printers, signatures, forms, communications equipment, telephones, etc and a source and alternative source defined;
• requirements for training and awareness of individual and group roles in disaster/contingency plan;
• testing schedule, results of last test, and corrective actions taken based on prior test(s);
• itemization of contracted service providers, services, and response expectations;
• logistical information on location of key resources, including back up site for recovery operating system, applications, data files, operating manuals, and programme/system/user documentation;
• current names, addresses, telephone/pager numbers of key personnel;
• reconstruction plans for re-recovery at original location of all systems resources; and
• business resumption alternatives for all users for establishing alternative work locations once information systems resources are available ie, system recovered at alternative site but user building burned to the ground and unavailable.

• Regulatory agency requirements with respect to contingency planning should be met.
• User contingency plans should be developed based on unavailability of physical resources for performing critical processing -- manual and computerized