As risk management tops the agenda could you survive an IT disaster?

The Combined Code of Corporate Governance places surviving an IT disaster firmly on the corporate agenda. One of the key points of the Combined Code is that the board is responsible for reviewing the effectiveness of risk management systems, at least annually, and reporting to shareholders that they are in place.

4-consulting director, Sandy Pratt, takes a look at the processes involved in completing an effective IT risk audit and developing a recovery plan, a task which becomes increasingly more complicated in a constantly changing environment.

IT Disaster Planning

All well-managed organisations should have plans for minimising the disruption to their operations and customer services when hit by some unplanned, sustained problem that affects a significant part of the business. These plans are usually described as "business continuity" plans. One of the most important aspects of the business continuity plan is the IT Disaster Recovery (“DR”) Plan.

The IT DR Plan usually involves a significant amount of technical effort to devise and normally involves some capital expenditure. As a result, the complete commitment of the chief executive and the senior management team is essential. Once written, the plan must be kept up-to-date regularly. Organisations must be prepared to test their IT DR plans; without testing, the plans are worthless. Unfortunately, like any insurance policy, you never need it until you need it. As a result, the benefits are often difficult to perceive.

DR planning comprises a number of aspects including risk analysis (i.e. likelihood and impact cost), risk minimisation (i.e. contingency planning), risk transfer (i.e. insurance); and risk management (i.e. recovery prioritisation and planning). Each of these aspects is dealt with below.

Risk Analysis

Normally, the DR planner starts by considering the threats and risks that might impact on the organisation's IT facilities. These are often categorised into environmental, natural hazards, people induced and mechanical failure. These risks are then graded according to the likelihood of occurrence. For each risk, the planner assesses the magnitude of the impact. The combination of likelihood and magnitude enables the DR planner to identify those risks that require the most attention.

Risk managers often use a scoring system based upon “percentage of likelihood” multiplied by the financial value of the impact. However, effective assessments can be made by using scores of 1 (low) to 3 (high) for both likelihood and impact.

Risk Minimisation

It is good practice, when drawing up disaster recovery plans, to consider what actions can be taken to minimise the risks of disaster occurring. Each aspect of the technology used by the organisation should be examined to see how its resilience and redundancy could be improved. For example:

- by providing additional "fall-back" telephone lines,
- ensuring that spare network servers are allocated either within the organisation or on standby with a supplier,
- ensuring that alternative power supplies are available or
- installing spare "swappable" disk storage or other back-up devices.

Risk Transfer

It is common for organisations to take out insurance policies covering the risks associated with IT disasters. These policies usually fall into three categories - replacement of equipment, reinstatement of data and applications, or increased cost of working. For each; different scenarios should be examined.

Risk Management

Managing the risk comprises two separate functions. These are:

- Prioritisation of the order of recovery of business processes and
- Planning the recovery of each IT service

These are identified below.

Prioritising the Recovery

Once the various risks have been identified and their impact assessed, the DR planner must consider the importance of each part of the business. This identifies the related IT services that have to be restored and leads to the order in which they should be restored. This process is usually done by inviting each business department to identify which of their "line of business" applications they can operate without before there is a significant decline in the quality of service. Department managers should also be asked to prioritise the recovery order of each of these applications. Any associated timescales would be helpful to build a complete picture.

These various responses are collated and an overall set of restoration priorities and timescales established. Usually, the critical issues revolve round the questions:

- How do we continue to service our customers?
- How do we continue to pay our suppliers?
- How do we continue to pay our staff?
- bullet
- How do we continue to collect our debts?
- How do we track our liabilities?

Only when the priorities and required restore times have been agreed with the business managers, can the IT DR planner move on.

Planning the Recovery

In drawing up plans for recovery, the DR planner normally assesses plans for a variety of disaster scenarios. These can range from total loss to loss of selected assets or the unexpected failure of a key piece of equipment.

For each scenario, the DR planner must define clearly the scope of the plan. The scope can cover locations, applications or simply equipment. For example, disaster recovery plans might be developed separately for Head Office and for Branch Offices.

Each scenario should be separately documented. The IT disaster recovery plan should describe the scenario and the associated activities and technology that are in the scope of the plan and those that are excluded from the plan.

The plan should include a general overview of how the organisation will restore its IT services in each case. The plan should also include an explanation of the recovery management framework describing the various members of staff that constitute the recovery team, their roles and the reporting lines.

A well-written IT DR Plan will contain sets of work instructions that should be followed in order to reinstate each item of equipment, each application and each data set associated with the disaster scenario.

The aim of an IT Disaster Recovery Plan is to avoid the recovery team having to ask questions or resolve technical problems that could have been foreseen. By thinking through the process in advance, the need to take decisions under stressful conditions, with the obvious risk of mistake, can be avoided. It is therefore the essential that each IT Disaster Recovery Plan is thoroughly tested and, where problems are identified, appropriate contingency measures taken and the recovery plans modified.

Finally, it will be necessary to assess the internal competencies within the business. In this way, it will be possible to understand and to plan for when external assistance will be necessary and to decide who might fill any skills gap. The likely costs associated with any additional assistance can be identified and included within the assessment.

Recent changes to corporate governance guidelines, including requirements for risk assessment statements in the audited accounts, require chief executives and company directors to take responsibility for the proper management of risk within their organisations.

For more information on the sort of risks your organisation might face, the possible solutions and associated costs, email Sandy Pratt of 4-consulting at Sandy.Pratt@4-consulting.com for one-to-one advice.

Sandy is an experienced advisor on DR Plans and has developed plans for many businesses including a Scottish economic development agency, a UK public utility company and an international oil services company.