Disaster Recovery Planning

Welcome to this lecture (slides with voiceover) on disaster recovery plans. We saw in the previous lecture the relationship between a business continuity plan and disaster recovery. In this lecture we will look at disaster recovery in more detail.

The main objective of a disaster recovery plan is to prepare and be ready for any disaster that might occur and before it occurs as it mitigates both the short and long-term damage. It may be noted that Fault Tolerance and Disaster Recovery Plans are different. Difference being that fault tolerance is concerned with enabling increased availability of systems in the occurrence of an isolated outage, and DRPs provides the procedures to recover systems from outages after a major failure.

Let us re-cap on the previous lecture where we highlighted the purpose of a business continuity plan a (BCP),that is keeping business operations running after a disaster has occurred. A disaster recovery however, is concerned with restoring business operations after the said disaster occurrence and getting the business operations back to normal. There are some common elements with the BCP and DRP in that they both deal with identifying critical business functions, and possible scenarios. We have been introduced to these scenarios in previous lectures where they are envisaged by the planning team who assess the probability and possible impact of events on an organisation occurring. Another common element - 'experts' who understand the organisation's critical business processes. Both the BCP and DRP engage with different activities and both start at the same time and have the same goal; that is to provide plans for the long-term survival of the business.

There are a number of elements to a disaster recovery plan (DRP), and we will be looking at these in more detail throughout this lecture. What we see on this slide are a few essentials that are needed. For example, primarily the damage incurred has to be assessed for any damage to buildings and equipment and procedures to carry this out have to be documented. This entails the response team determining which assets are totally lost, which can be retrieved and repaired, and which remain usable. The damage may be so that new sites have to be investigated to continue operations.
The primary objective of the DRP is to restore all work operations and facilities with their required assets. To respond to a disaster occurring, all personnel need to respond effectively and an awareness of these plans is crucial to the recovery of the business. This means that training and awareness has to be given to all concerned. The plan has to be of high quality, with feasible disaster recovery procedures and needs to be kept up to date.

We already know that a Disaster Recovery Plan (DRP), includes a number of policies and documentation in order to respond to a disaster where business operations are affected. In the last lecture, we looked at Business Continuity Plans (BCP), and Business Impact Analysis and their respective purpose and roles. The BIA drives the requirements for the BCP and consequently in turn, the BCP drives the requirements of the DRP.

When developing disaster recovery plans, a primary task is to define the disaster recovery objectives and the purpose and scope of the plan, and which disasters they will focus on. The plans include *"detailed steps and procedures that identify how to recover the organisation in response to a disaster."* Identifying Critical Success Factors (CSFs) are also essential. Management support is needed and the developers of the plan need to have the relevant standard of knowledge and authority to proceed with the plan. As we saw previously, alternate locations may be needed and of course have an adequate budget. On completion of the plans, regular review and testing has to be carried out to ensure they are fit for purpose and kept up to date.

The disaster recovery plan has to be fit for purpose and any updating or upgrading of IT systems changes have to be documented. We saw in a previous lecture, the importance of employing change management processes to ensure that there are no knock on effects from these. The plan developers should be updated with any of these changes to assess if any impact on the plan itself. On this slide, we see the elements that

should be included in a DRP review as well as best practice for its implementation which summarises the details of a DRP.

Firstly, systems should be verifies for those covered by the plan to assess if any changes have been made. Critical business functions should be identified to verify the plan covers these adequately and that priorities have not changed. Alternate sites have to be investigated in the case of the site being inadequate for the business purposes. Contact information must be correct in order for relevant parties to be notified. The best practices as identified by Gibson and Igonor are that it must be assured that BIAs identify the critical business factors which are in turn used to identify the critical business operations and critical servers and services. It is essential in any plan to have a clear purpose and scope in order to stay focused and develop a plan that is fit for purpose. Reviewing and updating the plan are essential activities in order for it to remain adequately effective and fit for purpose. If critical systems are changed than any impacts on the plan should be adequately addressed. Testing is essential as it ensures the plan can be implanted as expected.

In summary, the preceding slides are an overview of Disaster Recovery Plans. Now please take a break and reflect on what we have learned so far before moving on to the next task which is to read Chapter 14 of the core module text which will enable you to gain a more in-depth understanding of disaster recovery planning.