12.2 Disaster Recovery

A disaster is any event that significantly disrupts your organisation’s operations. A hard drive crash on a critical server is a disaster. Other examples include fire, an earthquake, your telecom provider being down, a labour strike that affects shipping to and from your business and a hacker deleting critical files. Just keep in mind that any event that can significantly disrupt your organisation’s operations is a classed as a disaster.

12.2.1 Disaster Recovery Plan

You should have a disaster recovery plan (DRP) in place to guide the return of the business to normal operations. This must include a number of items. You must address personnel issues, which means being able to find temporary personnel if needed, and being able to contact the personnel you have employed. It also includes having specific people assigned to specific tasks. If a disaster occurs, who in your organisation is tasked with the following?

- Locating alternative facilities
- Getting equipment to those facilities
- Installing and configuring software
- Setting up the network at the new facility
- Contacting staff, vendors, and customers

These are just a few issues that a disaster recovery plan must include; your organisation may have more issues that would need to be addressed during a disaster.

12.2.2 Business Continuity Plan

A business continuity plan (BCP) is similar to a disaster recovery plan but with a different focus. The DRP is designed to get the organisation back to full functionality as quickly as possible. A business continuity plan is designed to get minimal business functions back up and running up to a certain level in order to conduct some type of business.

An example would be a retail store whose credit card processing system is down. Disaster recovery is concerned with getting the system back up and running at full functionality, essentially like the

disaster never happened. Business continuity is concerned with simply offering a temporary solution, such as processing credit cards manually.

To successfully formulate a business continuity plan one must consider which systems are most critical for your business and have an alternative plan in case those systems go down. The alternative plan does not need to be perfect, just fully functional.

12.2.3 Determining Impact on Business

Before you can create a realistic DRP or BCP you have to conduct a business impact analysis (BIA) of what damage to your organisation a given disaster might cause. Consider a web server crash. If your organisation is an e-commerce business, then a web server crash is a very serious disaster.

However, if your business is an accounting firm and the website is just a way for new customers to find you, then a web server crash is less critical. You can still do business and earn revenue while the web server is down. You should make a spreadsheet of various likely or plausible disasters and conduct a basic business impact analysis for each.

An issue to consider in your BIA includes the maximum tolerable downtime (MTD). How long can a given system be down before the effect is catastrophic and the business is unlikely to recover? Another item to consider is the mean time to repair (MTTR). How long is it likely to take to repair a given system if it is down? You must also consider the mean time between failures (MTBF). In other words, how frequently does this particular service or device fail? These factors help you to determine the business impact of a given disaster.

All of this data will lead you to a recovery time objective (RTO). That is the time by which you intend to have a service back up and running, should there be a failure. This should always be less than the MTD. For example, if the MTD for your e-commerce server is 48 hours, your RTO might be set at 32 hours, providing a significant margin of error.

Another important concept is recovery point objective (RPO). This is how much data you can tolerate losing. Imagine you do a backup every 10 minutes. If the server you are backing up fails seconds before the next backup, you will have lost 9 minutes and about 55 to

59 seconds of work/data. That will all have to be redone manually. Is this tolerable? That depends on your organisation.

12.2.4 Testing Disaster Recovery

Once you have both a DRP and a BCP, you need to periodically test those plans to ensure they will actually work as expected. There are five types of tests in order, from the least intrusive, easiest to conduct, to the most difficult and the most informative.

12.2.4.1 Document Review/Checklist

This type of testing is usually done by an individual. The BCP and/or DRP are simply reviewed to see if everything is covered. They are compared to check lists and perhaps check lists from various standards (like PCI).

12.2.4.2 Walkthrough/Tabletop

This is a team effort. A team sits in a conference room and goes through the BCP and/or DRP and discusses scenarios. For example, “What if there was a fire in the server room?” Then the plans are consulted to see if that is covered adequately and appropriately.

12.2.4.3 Simulation

The purpose of this type of test is to simulate some sort of disaster. A team or an individual might conduct this type of test. It involves moving around in the organisation and asking specific individuals “what if” scenarios. For example, you might ask the database administrator “What is the plan should our financial data server crash now?” The purpose of this is to see if everyone knows what to do in case of a disaster.

12.2.4.4 Parallel

This test is about seeing if all backup systems come online. That would include restoring backup media, turning on backup power systems, initializing secondary communication systems, etc.

12.2.4.5 Cut-off/Full Interruption

This is the ultimate test. You actually shut down real systems and see if the BCP/DRP works. From one perspective, if you do not ever try out

this level of testing, then you do not really know if your plans will work. However, if this goes wrong, then you have just caused a disaster.

To avoid generating a disaster, there are certain steps you can take. Firstly, do not even consider this test until you have successfully completed the previous tests. In fact, all of these tests should be done in order. First, conduct a document/check list. If only this is successful, then move to a tabletop. Then if that works move to a simulation.

Secondly, you should schedule this type of test during downtime for the company. To be more precise, it is better to do the test at a time that even if things go wrong, it will cause the least impact on the business. For example, if this is a bank, then do not carry out this test Monday morning. Perhaps Saturday afternoon would be best. This would give you a chance to fix anything that could potentially go wrong.