Presentation

Introduction

I was until recently one of the unseen people who would get the call at 3 am when there was a problem, so I am in a good position to tell you about disaster recovery from a real-world perspective. Working in a large multinational bank provided the opportunity to see these principals implemented at a very high level.

All business should have a general IT Policy, however basic. For purpose of this talk we will focus on disaster recovery. While important, hardware is becoming less relevant in today's environment, your company's greatest asset is your data.

"It can and will happen to you" Remember these words.

What is a disaster? Any event which will negatively impact the business' ability to function.

- User actions
- Equipment failure
- Cyber attacks
- Fires/Flooding
- Natural disaster

Basic policy should cover these questions:

- How do you safeguard your data?
- Who does what and when?
- What do you do in event of a failure?
- How long will it take to restore business functions?
- Do you test your plan?

Disaster preparedness is the fundamental aspect of the plan, and relates to your routine activity. As part of the plan you should have a comprehensive backup regime. If a server is present in the environment this is paramount, as it holds the bulk of your company information. Desktops, laptops and mobile devices are less critical but should be considered. Should a user device fail, how easily can that user be put back into production.

Backup regime should include three levels.

- Local backup, which is easily accessible for minor incidents such as restoring 'lost' files.
  - Backup is first step and needs to be regularly verified as successful
- Offsite backup to ensure data is secured in the event of damage to the premises.

- Remote backup is recommended where data is secured outside your geographic location, in case of major events such as natural disasters.

Disaster recovery (DR) lists the protocols in place to handle a catastrophic failure. Server or communications device failure is a major concern. How soon can you replace or resolve a failing device and restore the data if required. Where and what is the state of your backup medium, how easily is it accessed?

Business continuity Plan (BCP) defines how the business will operate during and immediately a disruption. How do you remain in contact with your staff and clients? How will you access your data? Where will you operate in the interim? As part of the protocol testing is necessary to ensure these plans can be implemented, particularly on short notice.

Ensure provider can provide hardware support in event of disaster recovery event

Overview of technologies

PowerPoint presentations with broad descriptions of technologies available and how they may be utilized in MSB scenario.

Brief Case Studies and Scenarios

- Examples of DR and BCP protocols
    - Major financial institutions
- Examples of worst case episodes
    - Small businesses encountered

Q&A