Disaster Recovery.

How to Create a Robust Disaster Recovery Plan.
Today’s agenda

✔ The drivers behind a DR Plan
✔ Disaster Recovery Fundamentals
✔ Risk analysis for Small Business & NFP
✔ Steps to build a robust DR Plan
✔ How cloud computing can help
✔ What’s Next?
“Let’s get to know you. Please help me by answering a few questions…”
Our Disaster Recovery Plan Goes Something Like This...
Main drivers of a DR Plan

1. Prevent loss of Data (Protection of intellectual property)
2. Restore your system in a timely fashion (Business continuity)
3. Compliance (e.g. board compliance, tender processes & government requirements)
DR Fundamentals

1. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

2. Recovery Classes

3. 7 tiers of Disaster Recovery
Key Measures - Time and Data!

Recovery Point Objective (RPO)

- How much data can you afford to lose?

Recovery Time Objective (RTO)

- How much time your business can survive?

10 am Disaster Strikes
## Where is your business situated?

**Recovery Time Objective (RTO) and Recovery Point Objective (RPO)**

<table>
<thead>
<tr>
<th>Class</th>
<th>RTO</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RTO</strong></td>
<td>72 hours to 1 Week</td>
<td>8 hours to 72 hours</td>
<td>Less than 8 hours</td>
<td>0 minutes</td>
</tr>
<tr>
<td><strong>RPO</strong></td>
<td>Last full backup - Less than 1 week</td>
<td>Last backup - less than 24 hours</td>
<td>Less than 15 minutes before the event</td>
<td>0 minutes</td>
</tr>
</tbody>
</table>

(https://en.wikipedia.org/wiki/Seven_tiers_of_disaster_recovery)
## 7 tiers of Disaster Recovery

<table>
<thead>
<tr>
<th>Tier 0</th>
<th>• No off-site data – Possibly no recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>• Data Backup with no hot site</td>
</tr>
<tr>
<td>Tier 2</td>
<td>• Data backup with a hot site</td>
</tr>
<tr>
<td>Tier 3</td>
<td>• Electronic vaulting</td>
</tr>
<tr>
<td>Tier 4</td>
<td>• Point-in-time copies</td>
</tr>
<tr>
<td>Tier 5</td>
<td>• Transaction integrity</td>
</tr>
<tr>
<td>Tier 6</td>
<td>• Zero or near-zero data loss</td>
</tr>
<tr>
<td>Tier 7</td>
<td>• Highly automated, business integrated solution</td>
</tr>
</tbody>
</table>

Source: [https://en.wikipedia.org/wiki/Seven_tiers_of_disaster_recovery](https://en.wikipedia.org/wiki/Seven_tiers_of_disaster_recovery)
Recovery Time versus Cost

Source: https://en.wikipedia.org/wiki/Seven_tiers_of_disaster_recovery
Developing the plan. Key Steps.

1. Risk & Impact Assessment
2. Develop the Execution Plans
   - Action Plan
   - Communication Plan
   - Detail Recovery Plan
3. Test
4. Post Actions
Risk & Impact Assessment

a. Identify most important business functions => Pinpoint the IT system and assets that support these functions.

b. Examine threats and vulnerabilities (internal & external) that will severely impact the company’s ability to conduct business:
   - Loss of data (e.g., Server failure, accidental or deliberate deletion)
   - Loss of IT function (e.g., Computer virus, vendor out of business)
   - Loss of skills (e.g., accidents, illness)
   - Loss of access (e.g., Fire, flood, extended power outage)

c. Determine the risk factor by assessing:
   - Likelihood of occurrence
   - Impact to business
Risk Factor Matrix

High Risk (Likely)

High Impact to Organisation

Plan

Prevent

Likelihood

Low Risk (Unlikely)

Low Impact to Organisation

Accept

Contain

Impact

Eg. Have a plan B

Eg. build some redundancy

Eg. communicate situation with stakeholders

Eg. education & incremental improvement

High Risk (Likely)

Low Risk (Unlikely)
Developing the Execution Plans

1. Define your action plan
   - Minimum number of core staff to conduct business
   - Minimum technology to conduct business
   - Determine priority of recovery

2. Communication Plan
   - Who is in charge of communication
   - How to reach your staff, customers and suppliers and inform them of the situation (you may have no access to emails and contact lists)
Developing your DR plan cont’d

3. Detail Recovery Plans

- System specification
- Warranty & vendor support information
- Support contact information
- Dependencies (hardware, software, licenses, backup)
- Recovery Procedure – the steps and estimated time to perform the recovery.
After the Plans

1. Identify components where you may do a test-run.
2. Identify the gap for input into the next IT Strategy Plan.
3. Store your DR plans offsite.
1. Be realistic, start with a simple plan and build on it over time.

2. Focus on the most critical components in your business.

3. Think outside the box.
Can cloud computing help?

1. Data Centers are equipped with redundancies (power, hard disks, servers, internet links) and offer ideal operating environment for computing devices (dust free, constant temperature and humidity).

2. Simplify your infrastructure and therefore inherently reduce your overall risk.

3. Choose reputable cloud solution providers.
To summarise......

1. Recovery Point Objective (data) and Recovery Time Objective (time)
2. Risk & Impact Assessment – assess likelihood and impact of risks
3. Execution plans – action plan, communication plan and detail recovery plan
4. Identify gaps for consideration in your next IT plan
5. You can develop your DR plan on a limited budget & resource
6. Consider cloud technology as part of your DR solution
Contact me on 1300 89 22 00
Or Email carlson@itconnexion.com
http://www.itconnexion.com/
... AND WE'RE DONE!

Any questions?