

Business Continuity Planning

1 RISK ASSESSMENT

1.1 SUMMARY

Before planning the disaster recovery options, we need to understand where the vulnerabilities lie, what the priorities are and what the financial implications are.

This analysis requires a breakdown of the business into components, so that we can understand what the elements are and to profile them to understand costs, sensitivity, alternatives and the people and resources that each part relies on.

1.1.1 BUSINESS DEVELOPMENT

Our CRM systems hold the 'pipeline' of future work and are vitally important. We hold information about our prospective client needs in our CRM and in our email, and for us to be able to maximise our ongoing potential, we need to maintain this data. The impact of a disaster on the 'new business' of a firm is limited to the effect reputation.

| Resource | Impact | Cost per hour of downtime | Sensitivity to downtime | Alternatives |
|----------|--------|---------------------------|-------------------------|--------------|
| eMail | | | | |
| CRM | | | | |
| | | | | |
| | | | | |
| | | | | |

1.1.2 PROCESSING BUSINESS

Our daily workloads are vulnerable to a disaster. Timelines are tight, and the effect of failing to achieve one can be severe. Our projects all have deadlines that could be at any time, most likely at the end of a day, and all with implications if they are missed.

Meeting these deadlines requires the following resources:-

| Resource | Impact | Cost per hour of downtime | Sensitivity to downtime | Alternatives |
|----------------------------------|--------|---------------------------|-------------------------|----------------------------------|
| eMail | | | | |
| Document Management | | | | |
| Production Planning Spreadsheets | | | | |
| Printers / MFCs | | | | |
| Stationery | | | | |
| PDF generator | | | | |
| Landlines | | | | Divert main lines to cell phones |
| Cell Phones | | | | |

| | | | | |
|--|--|--|--|--|
| | | | | |
| | | | | |

1.1.3 MANAGING THE BUSINESS

There are a number of tools required to manage the businesses day to day operations. These include

- Phone Management Software
- HR /Payroll
- General Ledger
- Building Security

The impact of these being unavailable is

1.2 INFRASTRUCTURE

To support the items above, the following shared services are also used

| Item | Supports | | | Accumulated cost of outage per hour |
|-------------------------|---------------------|--|--|-------------------------------------|
| Utilities | | | | |
| Electricity | All | | | |
| Water | Staff | | | |
| Internet | IRD, Banking, eMail | | | |
| Network Services | | | | |
| Network Firewall | | | | |
| Network Switches | | | | |
| eMail Server | | | | |
| AntiSPAM | eMail | | | |
| Login Server | | | | |
| PMS Server | | | | |
| Database Server | | | | |
| Phone System | | | | |
| Voice Mail Server | | | | |
| Call Logging Machine | | | | |
| UPS | | | | |
| | | | | |
| | | | | |

2 PLANNING

Disasters come in all sizes, from being a specific item of equipment (a failure), a number of items (e.g. a small fire or flood), office wide or much larger scale like the recent Christchurch earthquake. The most common disasters are the smaller ones and the least likely are the large scale events. In a large scale event, there would be unique challenges competing for resources with other businesses, and more importantly, for staff to manage in their private lives.

The purpose of this document is to identify a number of resources and make these available to the recovery teams, equipping them with the best possible toolkit to recover business processes quickly. The priority is set above, by understanding the most urgent or impactful services, and working through the items they depend on in a logical order.

Steps include

- Disaster Prevention
- Disaster Work-around (quickly achieving limited capacity of key services)
- Recovery (returning services to normal)

The following steps are in place

2.1 DISASTER PREVENTION

Power – UPS (tested)

IT Protection - Virus/SPAM/Firewall

Water – bottles?

Security – (physical)

2.2 WORK AROUND

Remote Access – access what items from where? E.g. Recovery to a data centre, or have arranged loan equipment (add details)

Mobile data cards

Warranty details

Support contracts

Spare equipment

2.3 RECOVERY

Backups

Options for recovery (including premises and ability to obtain necessary equipment)

Warranties

Insurance

2.4 COMMUNICATIONS

In the event of disaster, we are committed to communicating too key stakeholders and keeping them appraised. The communication will be managed by or, in their absence, by

| Stakeholder | Immediacy | Message | Method |
|-------------------------|--------------------------------------|---|--|
| All staff | Within xx of detecting the problem | Who should be in the office Who should leave the office Overview Expected timeline Expected recovery plan Refresh every xx hours | Phone/Text (need a current list of all cell phone numbers) |
| Key clients | ?? | Brief outline Impact on the client Expected timeline | Letter/Email/Phone? |
| Insurer | | | |
| Bank | | | |
| Phones | | | |
| ICT Provider (Kinetics) | Immediately on detecting ICT problem | Request assistance | Call 0800 Kinetics, If after hours, follow the menu. Or ring Andrew Hunt on 021 610066 |
| | | | |

2.5 DELEGATED RESPONSIBILITY

Disasters seldom occur at convenient times. Key personnel may be unavailable. This is overcome by establishing a ladder of contacts and delegated authority/decision making

| Order | Person | Area of Responsibility | Upgraded Delegated Capex Approval |
|-------|--------|------------------------|-----------------------------------|
| | | | |
| | | | |
| | | | |
| | | | |

3 TESTING

How will we verify the plan?

3.1 SCHEDULE FOR TESTING

Partial tests covering ... will be run every ...

Full tests covering .. will be run every ...

3.2 CRITERIA FOR ESTABLISHING SUCCESS/FAILURE

3.3 THIRD PARTY VERIFICATION

The plan was reviewed by on and they provided the following comments that have been incorporated into our plan.