Global Information Assurance Certification Paper

2003: A DR Odyssey

By Jane Whitgift

November 2003

GSEC Practical Assignment 1.4b

Option #2

ABSTRACT

The DRP for site-x needed to be updated. As Hussong identifies

"The plan is the organization's strategic battle plan for recovery. The follow-on contingency plans of the operating elements become the organization's tactical battle plans for survival.

BUT FIRST, THE CONCEPT

There are no permanent solutions, only evolving answers!"

Just because there is no commitment from the businesses for continuity planning there is no excuse for the IT department to neglect its duty in preparing a DRP. This case study outlines the site-x DRP project and the evolution since completion. It examines the issues that need to be addressed by the project; follows the project through the various stages in the DRP project lifecycle, identifying the issues addressed and lessons learnt in developing the DRP and concludes by outlining the difference the project has made to DRP in site-x.

Table of Contents

1 Before - site-x

The DRP

Following a reorganisation of the IT department at site-x, I was nominated as the IT Disaster Recovery Plan (DRP) owner – "there is a copy somewhere on the intranet" was not a promising start. The DRP had been written in 1995, published and long forgotten. Since being written, the business activity carried out at site had changed, the IT infrastructure had evolved, and the IT organisation had changed. The DRP cited organisations that no longer existed and people who had changed jobs.

The DRP is the contingency plan for the IT services to be invoked when normal IT services are severely disrupted. The plan outlines how to provide contingency services and plan for restoration of normal IT services. In many respects it is the response to the requirements for IT services defined in the Business Continuity Plan (BCP)

Issues:

1) The existing DRP was several years out of date.

The state of business continuity planning

Contingency planning is a business issue rather than a data processing issue. In today's environment, the effects of long-term operations outage may have a catastrophic impact. The development of a viable recovery strategy must, therefore, be a product not only of the providers of the organization's data processing, communications and operations centre services, but also the users of those services and management personnel who have responsibility for the protection of the organization's assets.(Computing & Networking services, University of Toronto)

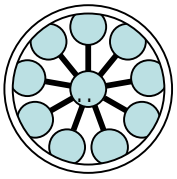
Where there are multiple businesses depending on a common infrastructure it becomes increasingly important that the distinction between the BCP and the DRP is understood. The BCP is the plan written by the business to enable management to understand what they will do to ensure continuity of critical business processes in the event of an incident disrupting normal services. The BCP should document which business processes are critical to business success including an understanding of when each process becomes critical and the resources required to support it. Simply documenting the requirements, or assumptions, of service availability is not sufficient, there must be conversations with all the teams supplying services to understand what services can be delivered during scenarios considered for the BCP. Any gaps in requirements and ability to deliver services must be identified, for each gap identified the business teams must decide to either accept the risk (this may require a different BCP or a fundamental change in how the process is delivered) or enhance the provision of service (for IT this will inevitably require an IT project with associated costs).

Issues:

2) Within the company, each business leader is responsible for creating and maintaining a BCP for their business. To date, development of BCP has not been given proper consideration by the businesses based in site-x with the consequence that no BCPs exist for these businesses.

Company structure

Fig1: Company structure



The company is organised as a federation of businesses split by market sector and region reporting into a Head Office. Individual businesses have freedom to operate within the framework defined by Head Office. The framework defines overall company strategy, business ethics, total expenditure, standard business processes for reporting into the HQ, and standards for cross business functions e.g. HR and IT. Within each of the businesses there is a manager who has accountability for IT services (BITM); this individual is the main contact point for the IT organisation into the business.

One of the company's major business centres is site-x, hosting about 2000 users from 40 businesses. The office complex consists of seven separate buildings. The computer rooms are all located on the ground floor of one of the buildings: building 101.

Issues:

3) Each business has different business processes and priorities and can determine levels of acceptable risk to their operation, leading to conflict in IT service provision at site.

4) Many of the Business teams are split across multiple sites with team use of IT infrastructure split across multiple sites, the scope for a DRP project could encompass all IT infrastructure in the company

IT services delivered from site-x

Following an aggressive outsourcing strategy the majority of the IT support teams have been outsourced.

Issues:

5) IT system documentation is scanty as either documentation has been misplaced following transitions of support teams or cost cutting during the final stages in projects resulted in systems documentation not been created.

Each company site has its own infrastructure for the IT services required by the business users on site. There is rarely shared infrastructure between sites and the infrastructure is generally running at approx 90-95% capacity.

- Desktop & applications

The company has a standard build for desktop machines which is based on the Microsoft Windows 2000 operating system and Microsoft Office 2000. Business teams share data files either on shared areas on file and print servers or using web based technologies on the company intranet.

The company has standardised on two operating platforms for applications. The majority of business applications are run in an NT environment. There are specialist applications running in a UNIX environment.

- Telephony

There are a large number of telephone lines entering site-x. At the start of the project all telephone lines went through a single sub-station. There are few lines direct to desks, most go to one of two Hicom telephone switches. Both switches were located in the same telecoms room.

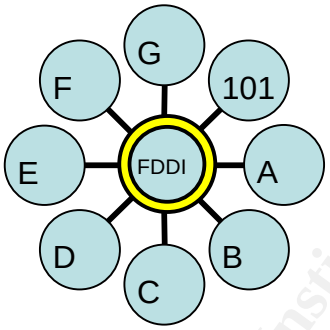
Issues

6) Single point of failure with the telephone supply to site

7) Single point of failure with both telephone switches in same room.

- Networks – WAN and LAN

The company sites are networked via private leased lines. Site-x was connected to one other large in-country site and one large overseas site, both connections were in the telecoms room. Some of the smaller company sites connect into site-x via a leased line; they generally also have ISDN backup terminating in site-x.



Site LAN design was a switched network. There was an FDDI ring in the server room and a single network connection from each server to the ring. The site was connected as a star topology, the FDDI ring at the hub with a single connection to each building from the computer room.

Fig 2 – Site-x LAN topology

Issues:

8) Single points of failure in connectivity to other company sites

9) Single point of failure for buildings on LAN

Risks to IT delivery

Items to consider in determining the probability of a specific disaster should include, but not be limited to: geographic location, topography of the area, proximity to major sources of power, bodies of water and airports, degree of accessibility to facilities

within the organization, history of local utility companies in providing uninterrupted services, history of the area's susceptibility to natural threats, proximity to major highways which transport hazardous waste and combustible products. (Wold & Shriver)

There have been a number of local incidents which have impacted service provision but fortunately causing little disruption to business:

- Utility failure :

  Gas Leak in telecoms provider manhole causing telephone outage for 4 days. This was off-site service interruption that we had no control over.

  Contamination in site water supply for 24 hrs in summer. Required water-cooled air-conditioning units to be switched off and therefore computer equipment had to be turned off.

  Heat wave causing the air conditioning to fail!

  Water leak from air conditioning unit in main Computer Room, damaging three servers.

- Staff unable to get to site: Fuel shortage caused by strike action of the tanker drivers. The site was within 24 hrs of being closed as food deliveries could not be made to site

- Small Fire in computer room through discarding a lighted cigarette in a wastebasket.

- Failure of one or more servers through hardware or software fault

The probability of being impacted by the local risks has not changed, however the global business environment has changed.

Following September 11 it is recognised that disaster impacting site and systems availability may be a deliberate attack rather than accidental. Media coverage of terrorist activity indicates that the general threat level has increased. Since September 11 the company has been at a high alert status.

Issues:

10) Increased threat level for deliberate attack of site-x causing damage to building and IT infrastructure

MessageLabs report that August 2003 is the record month for virus attack with 1 in 29 emails being infected. In the last two years there has been a significant increase in cyber attacks making national news headlines. As reported by MessageLabs

Sobig.F may have failed in its ultimate business objective, to create a network of spam sending machines, but the people behind these combined threats are using lessons learned from each attack to perfect their strategies. Attacks will continue until they prove successful.

Before 2001 there had not been a serious virus infection within the company. However CodeRed, Nimda, Slammer, SoBig and more recently Nachi have all breached the defences and caused disruption to business.

Issues:

11) Increased threat and potency of cyber attack as sophistication of attacks increases and business users become more reliant on IT for day-to-day activity.

IT continuity provision

Since the mid 90's there has been an increasing reliance by the business on IT services for day-to-day operations. Following several years of extreme cost pressures on the IT budgets, the businesses have requested removal of IT continuity provision costs from their budgets. The IT organisation has had to cancel all formal continuity provision.

There is an expectation within the businesses that, even following total destruction of the computer room and the entire IT infrastructure, all services would be available within a reasonably short time-frame. The expectation was that the project to procure, build, configure and load terabytes of data would be complete in a couple of months!

Business staff have become accustomed to being able to be flexible with their working arrangements, being able to work from other company offices, work while travelling and work from home. There is an expectation that if site-x is unavailable then staff will be able to continue business as usual by transferring to another site or working remotely from home. There is little recognition that if there is no infrastructure in site-x they have lost access to the IT services they use.

Issues

12) Although the business is increasing reliant on IT systems there is no formal IT continuity provision.

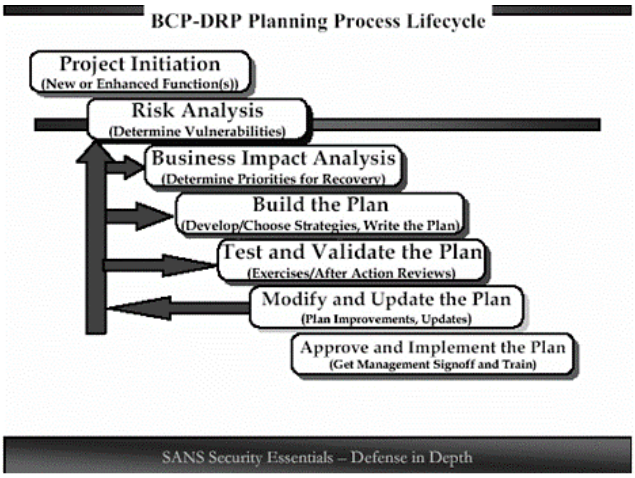
13) Unrealistic expectations of the IT services available following disruption of the IT services in site-x.

14) Unrealistic expectations of time scales for IT infrastructure projects.

2 During - The IT DRP Project

The project broadly followed the stages outlined in the SANS BCP_DRP Planning Process Lifecycle.

Fig 3 BCP-DRP Planning Process Lifecycle (Cole, Fossen, Northcutt, Pomeranz: p372)



2.1 Project Initiation

Agreement for project to proceed

Site-x has no history of serious IT incidents reinforcing the perception within the site-x businesses that continuity planning was a process that was not worth worrying about. The first step was to convince the BITMs that the current IT DRP was insufficient and that they needed to authorise a project to update it.

I held a meeting with the IT management team & the BITMs, the objective of the meeting being to obtain commitment to update the IT DRP. During detailed planning to understand how the meeting would reach its objective, I changed the format of the meeting. Initially I was going to invite a BITM from another site which had just completed updating its DRP to expound the benefits of having an up-to-date DRP. My breakthrough was a decision to hold a walkthrough using the existing DRP. The participants were asked to bring to the meeting the DRP and anything else that they thought would be useful in managing an incident.

Some of the participants were able to find a copy of the DRP, we had several different versions. No one was clear who should be doing what or when or what the options might be, but they were agreed that they were the people who should be managing the incident. By the end of the allocated time for the walkthrough there was general agreement from the participants that the site-x DRP was urgently in need of updating and authorised a project to update it.

The Project Scope

Before starting the project I needed to create clear boundaries for the project. The project was to create a DRP for site-x IT systems and improve the DRP position within 12 months. With this in mind the following parameters were set:

Business staff covered: The project is limited to cover the IT needs for process continuity of those business staff that are based in site-x. Where a team is split over multiple sites, only those processes that are covered by the team in site-x would be covered by this project.

IT services covered: There are many global teams and processes within the company, and teams are increasingly using services and applications which are based at other company sites or externally. This project would only cover DRP for IT services which are delivered from equipment based in site-x. Where IT services are used from other sites, where the service provider can be identified, the project will notify the relevant IT group of the site-x business dependence on its service. Where services have been externally purchased by the businesses it will be considered their responsibility to ensure there are the necessary continuity arrangements in place.

Criticality of IT systems: The project will concentrate on those IT services that are deemed to impact processes which will have a high impact to safety or company reputation or cost (impacting share price) if lost.

2.2 Risk analysis

Having identified the risks (see Risks to IT delivery

page 6) an indication of the probability of the incident occurring and the impact this would have had to be developed. This is not an exact science and I needed to come up with a relational rating system for probability and impact. When looking for investment for the project to improve the DRP situation I developed the following diagrammatic representation for the risks with indicative costs to provide continuity to address the issues.

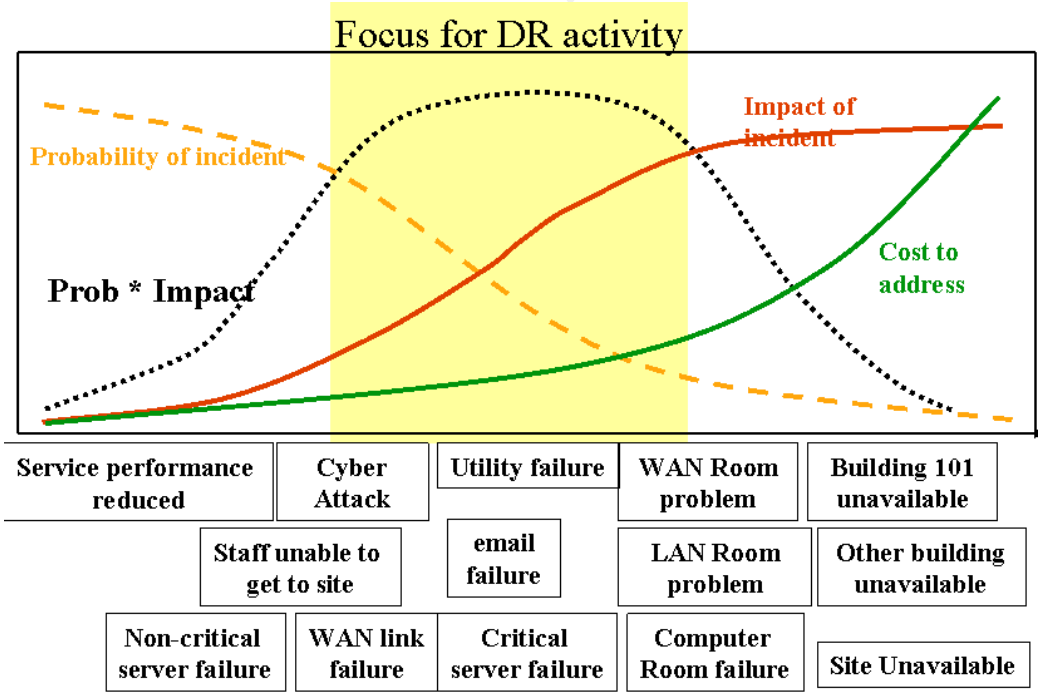


Fig 4 Risks facing site-x

2.3 Business Impact Analysis

I needed to be able to assess the impact of loss of the various IT services in order to understand what, if any, gaps in service provision there were. With the absence of BCPs, the pragmatic approach was to interview personnel within the businesses to understand the key processes and the IT services on which they were reliant. Working with the BITMs we identified the business personnel who needed to be interviewed. I engaged a consultant to help carry out a series of interviews to ascertain

- The key business processes, number of personnel involved and when the process was critical
- IT services on which the process relied, expectations of possible workarounds and impact of loss of service

This information was summarised on a form (see Appendix - A) and confirmed with the business representatives for accuracy. It was made clear that this was not their BCP but an indication of the IT services they thought to be important for their key processes and that it was a statement of requirements for services not what was available.

2.4 Choose the Continuity Strategy

Business Continuity Management: The improvement of an organisation's business resilience to the loss, disruption or interruption of its Mission Critical Activities their dependencies and single points of failure by providing for their continuation at an acceptable minimum level within the recovery time and recovery point objectives. This approach provides the three continuity strategies to enable an effective fit-for-purpose BCM capacity. (Smith (ed):50)

For each of the IT services delivered from site-x that were deemed to be critical by the businesses, I worked with the supply teams to propose options to improve the IT resiliency and continuity provision. I asked them to generate proposals with indicative costs for the identified options. I grouped the proposals into the following categories:

Do nothing

With the existing business framework it is acceptable for the businesses to decide that they wish to accept the risks associated with not having a DRP and any IT continuity provision. The risk associated with this option is that there could be no guarantees of being able to restoring any IT services due to limited system documentation being available.

Document & Resiliency

Increased IT resilience through small projects to improve resiliency of the IT services and creating IT documentation. There were two elements to the

documentation required. Firstly, creation of a complete set of documentation for the IT systems in site-x and secondly development of an incident management plan.

Detailed Preparation

Provision of IT continuity for critical IT services with minimal spend. The expectation was that this would be through development of a set of procedures and agreements with other company sites for temporary provision of services using their IT infrastructure.

Full Standby

Formal provision for IT continuity with options ranging from agreements with vendors to supply servers of defined specification at short notice, through provisioning of a backup site where there are servers available to restore backup tapes within a short timeframe, to a hot backup site where all data and applications are mirrored (providing almost instantaneous failover capability).

The Business Decision

The businesses in site-x needed to come to a collective agreement on the level of IT continuity they were prepared to fund. There were two factors that needed to be weighed up: the level of risk they were prepared to take and cost of the continuity provision. Recognising the business climate for cost reduction and therefore desire to minimise IT spend, I agreed with IT management that I should propose that the business approve a project to create documentation, increase resiliency and provide limited continuity using resources from other company sites.

There was commonality in the services the businesses deemed critical. In many respects the completed set of IT requirement forms made surprising reading. Whilst there are over 100 servers in site-x, the only IT services that were deemed critical were the email service for staff involved in critical processes, some of the team file sharing areas and some specialist applications based on UNIX.

For each of these services I developed graphs highlighting risk of the incident occurring, impact of service disruption and cost of proposed projects based on the risks identified in Fig 4 Risks facing site-x

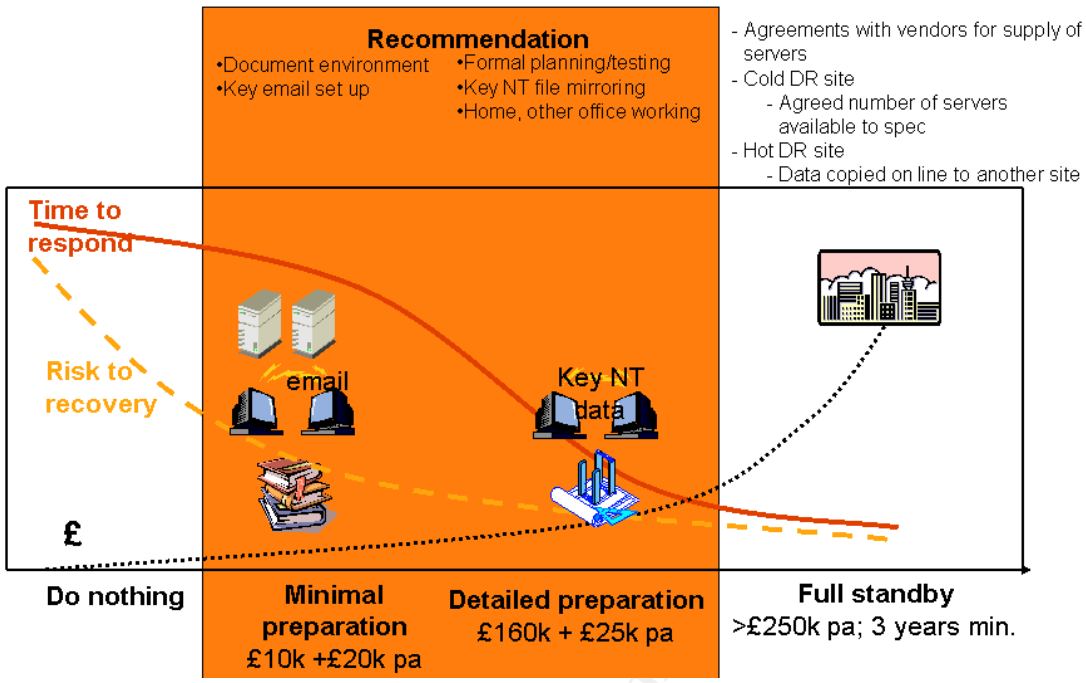


Fig 5 Proposal for improving DR provision for desktop services

The presentation to the BITMs included the risk to delivery (Fig 4 Risks facing site-x

a summary of critical systems from the Business Impact Analysis and proposals for improving DR provision for each of the critical services. This format was well received with a limited number of options for each service. BITMs approved the recommended projects for each of the services.

2.5 Building the Plan

This stage of the plan cycle had two elements, developing documentation and project managing the approved infrastructure projects to improve resiliency and provide continuity for critical services.

2.5.1 The incident management plan

The key elements of the Incident Management Plan include:

- Introduction
- Objective
- Formation of a IT incident response team
- IT incident response team organisation and responsibilities
- Document maintenance procedures
- IT DRP description

- Generic plan of action
- Reference documentation

Key observations and decisions made while creating the incident management plan and its evolution following lessons learnt during testing are noted below.

2.5.1.1 Formation of an IT response team – who, how, when

The site-x IT management team agreed that there should be a limited number of people who should be able to initiate the DRP. Recognising that incidents may occur at any time, we initiated the role of IT Duty Manager available 24by7, with associated rota of personnel manning the rota. Only those staff who are eligible to initiate the plan are on the rota.

There are many ways triggers causing an incident, and therefore many people at site-x that may inform the IT duty manager of a problem. To aid initiation of the DRP I decided to create a single telephone number that could be used to contact the IT duty manager. Use of a single number has advantages of

- There is no searching for lists of duty manager rotas and telephone numbers
- There does not need to be a published rota of duty managers, minimising the risk of other teams having an out of date copy of the rota.

Recognising that one of the problems could be a telephony problem at site, I asked to have the DR number created on a telephone switch at another site. The phone number has a "follow-me" facility enabling the number to be programmed to contact the IT duty manager either through their office number, or their mobile number or their home phone number. Many telco's now offer this service.

One of the first decisions of the incident manager is deciding if a team needs to be formed. I created the following table to provide a guide as to when the team should be formed and lists the factors to consider.

Form Team	**Example Incident**	**Factors to consider**
Declare incident internally	Computer room destroyed User building(s) uninhabitable	Number of Users affected Criticality of business Activities affected (Safety first)
	Power failure to Building 101 Services to building interrupted UNIX Service lost WAN link to operational sites lost	Impact on communication of incident to staff
USE PLAN..may need team	Staff unable to get to site Voice service lost Single WAN Data link down	Effectiveness of contingency Plans
	Service slow	Estimated time to re-instate full service
	Intranet failure	Confidence in solution(s)

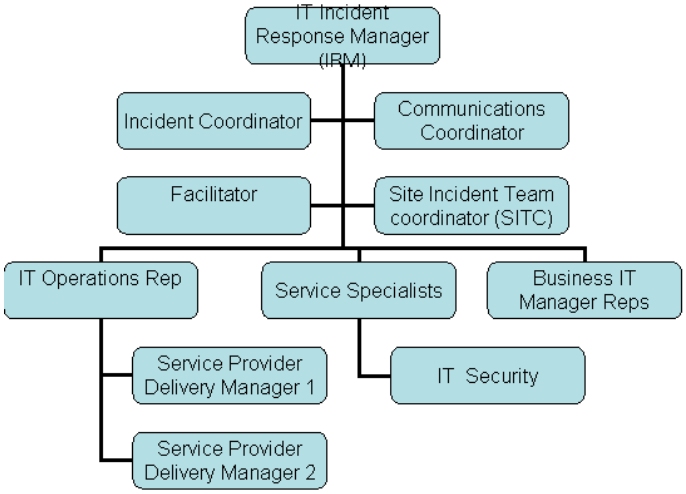
NO	Single non-critical server down Single non-critical application failure	Potential changes to impact

2.5.1.2 Roles and Responsibilities of Recovery Teams

The team required to manage an incident will depend on the nature of the incident. I created a team structure for the incident team that would cover the worst case scenario – the entire infrastructure at site-x was destroyed. I created a description for each role listing the key activities and tasks.

The incident team structure has evolved following testing to the following structure with recommendations on team composition and combining roles as follows:

Fig 6 IT Incident response team



Team composition

The initial meetings where the incident is being outlined and continuity options being developed should be attended by representatives from each of the businesses and representatives from all the support teams. The Incident Manager may not have a sufficient understanding of the services that are delivered by the support teams to accurately determine who needs to be involved in resolving the issues or services used by the businesses.

Following the initial meeting representatives may be stood down if there is no impact to the group they represent or they are not providing any of the services.

Roles and people filling the roles

The roles that are required for the incident team have been identified. Where there have been limited people available for a DR test, some of these roles have been allocated to the same person. The following combinations have been found not to work:

- Incident Response Manager(IRM) & Site Incident Team Coordinator(SITC)

  During early versions of the team structure, one of the IRMs tasks was to be the representative on the site incident team. The site incident team had a schedule of meetings and requirement for information feeds from IT. When the role was combined there were resource clashes as both teams needed input from the IRM. Splitting the role allows the IRM to focus on resolving the IT service issues, whilst there is still a single point of contact for the site team ensuring that there is a

consistent set of information being fed to the site team about how the incident is being resolved.

- Communications coordinator & IT incident coordinator

  The IT incident coordinator is required at all the meetings for the incident, and needs to follow up actions or brief people unable to attend the meetings. Developing timely communications cannot be done in conjunction with the documentation and action tracking requirements during the initial stages of an incident.

New Roles

The roles of facilitator and SITC have been added to the original team structure.

In the aftermath of an incident there is a tendency to want to dive straight into action, rather than taking the time to reflect and plan. The facilitator needs a good working knowledge of the DRP and assists the IRM assign roles and following the processes, ensuring that the team do not overlook critical elements of the plan.

The SITC is the IT representative on the site incident team. This individual needs a good knowledge of both the site incident plan and the DRP to effectively communicate between the two teams. They are the focal point of communication between the site incident team and IT response team ensuring information flow between the two teams is maintained

2.5.1.3 Plan Maintenance

Documenting the maintenance processes for the DRP makes it more likely that the DRP remains effective and fit-for purpose. The plan needs to be reviewed and updated at least annually and following any significant change for example

- Changes to a BCP
- New teams moving to site
- Changes in infrastructure
- Changes in role of any of the named individuals in the plan
- Following invocation of the plan so that lessons learnt during its use are incorporated

The extent of the changes required to the plan will depend on the detail included in the plan.

Locations of Documentation

There is little point in having documentation that is all kept at site and only accessible from the site. The primary form for the site-x DRP documentation would be electronic, with the preferred method of access being electronic.

I agreed that we would keep the following electronic copies:

- The master copy of the DRP is held on an externally provided web facing service. This enables the IT recovery team to access the plan from anywhere where there is internet connectivity.
- The IT Duty managers keep a synchronised copy of the plan on their laptops.
- A copy of the DR strategy and the main document of the incident management plan are available on the company IT intranet website which allows all site-x users to see the plan.
- A copy of all the documentation comprising the DRP is available on an internal fileserver assessable to all the IT staff working in site-x.

In order to manage the risk of computer virus we agreed that the IT Duty Managers would keep as copy of the Management plan in Hardcopy. The supporting documentation would only be available electronically.

Testing the DRP

The ongoing testing of the plan is as important element in maintaining the plan. As Rothstein says

"Top management must be made to understand that (1) an untested contingency plan is unlikely to succeed in an actual recovery; (2) testing (and, for that matter, plan maintenance) is an integral part of the plan development and implementation process, and not an option; and, (3) an untested contingency plan could, in an actual disruption, turn out to be dangerous as a result of unverified assumptions"

The annual test plan

The DRP contains an overview of the annual test plan. The objectives of the plan are to:

- Involve continuity requirements for all businesses on site
- Cover some element from all IT services and all supply teams
- Develop continuity planning options for services
- Integrate the site-x DRP with other continuity plans
- Test validity of assumptions
- Test continuity provision for new services

Planning the simulations

The most successful test of the DRP has proved to be simulation exercises. An outline of for planning the simulation is described in the plan and included below:

Preparation

- Advise all IT staff of the date of the exercise a month in advance. A meeting room is booked for the day but no incident meetings are pre-arranged. People are encouraged to carry out business and usual.

- There is no advance warning of details of the incident for any of the on-site staff. Where activities may require agreement from other sites for setting up IT services I get agreement from the relevant site managers.

- In the week before the exercise DRP training sessions are held outlining the DR strategy, the generic processes, the roles and describing the reference documentation.

On the day

- After the incident is initiated the plan is used as if it were a real event

- Business users are involved in the exercise by their BITM. Their input is essential to establish the current critical processes and IT support required.

- Following prioritisation of business requirements and understanding how IT continuity will be provided the exercise is generally concluded.

- The supply teams will complete the exercise by creating the IT service in the way developed during the exercise, testing assumptions e.g. backup capability, ensuring we do not fall into the trap cited by Delio

  "Ontrack (http://www.ontrack.com/), one of the best-known professional data restoration services, estimates that over 80 percent of its customers had backed up their data but were unable to access it when they needed to".(ref 6)

Post Exercise Reviews

The post exercise reviews are an important part of the DR exercises. The review is scheduled a week after the original exercise. All participants attend or submit their review. We follow a standard agenda

Summary of the incident

What we did do during incident?

What have we learnt about site-x environment?

What went well?

What could be improved?

Lessons learnt from the exercise are discussed and incorporated into the DR documentation and test program as appropriate.

An outline of some of the incidents that we have tested for is summarised below. The scope of the incidents is contained to allow us to focus on using the plan rather than the complexity of the incident and complete an exercise in a day.

Air conditioning fails

Scenario: Site services have given us 4 hrs warning that there is a problem with air-conditioning units and they need to be taken out of service. Site services have managed to find replacement machines but they only have half the capacity.

Armageddon Worm

Scenario: Cross platform worm has been developed that will propagate for 5 hours then cause damage to the operating system. The company has the vulnerability that will be attacked. At start of scenario the virus was not in the company network, four hours later it was first reported inside the company, five hours before site-x was impacted.

Server room fire

Scenario: Selective fire in the computer room that has damaged a subset of the IT infrastructure.

2.5.1.4 IT Disaster Recovery Plan Description

Outline Plan Description

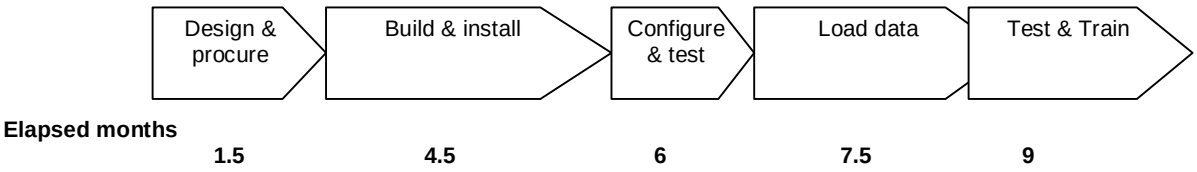


Fig 7 – Project timescale to rebuild infrastructure

The business expectation was that large infrastructure refresh projects could be completed within a matter of weeks. In site-x over recent years there have been a number of large infrastructure refresh programs which have demonstrated the reality of the timescale being closer to 9 months, and these started with a working computer room with network connectivity. These projects have proved invaluable in reminding the BITMs and business of the real timeframes to re-create the infrastructure.

Smith (p72) identified that there needs to be

"a framework that clearly identified and sets out time criticality, resources and actions"

Appendix - B contains the current framework for DR strategy for site-x.

Plan for Full recovery

The site-x IT management team agreed that we should not to develop a project plan for full recovery. This was a conscious decision as it was felt:

- There are many different scenarios in which services are lost, the criticality of the services change depending on the business cycle and hence the order in which services need to be re-established changes.
- There would be significant cost of maintaining the plan, with the possibility during cost cutting exercises this would be an easy target for cutting.
- The site-x infrastructure had evolved over a number of years. If starting from scratch the infrastructure could be optimised more effectively.
- With no supply agreements for equipment, the lead time for delivery of equipment would provide ample time to develop full project plans for build of the infrastructure.

Interaction with other plans

The DRP is unlikely to be the only plan that will be invoked during an incident. The linkages and interfaces between the IT plan and other continuity plans within the company need to be considered, e.g. site office accommodations plans.

Facilities during Incident

During the incident the incident team will need an incident response centre. Given the cost constraints site-x does not have an IT incident response centre permanently available either offsite or onsite. During development of the plan I identified a number of locations both on-site and off-site where the incident response centre could be set up, with informal agreements that this might be possible.

The preferred location for the IT Incident centre is a meeting room at site. I have established that the IT incident team has priority use of this room once an incident has been declared – and all know when they book the room that they might be evicted at short notice. The meeting room is set up with paper copies of DRP - this has proved invaluable at start of exercises.

A tool that has proved useful during exercises is use of telephone conferences, enabling meetings to be set up quickly without staff needing to travel. In order that telephone conferences can be quickly set up I have established two instant meeting (MCI) accounts for audio conferences that are available exclusively for use by the IT incident team. The data to access the conferences is published to all who might be involved in managing the incident and needing to attend audio conferences.

All IT systems that the incident team need to access need to be identified, e.g. document stores, procurement systems. Many systems require pre-registration before they can be used, and rarely is registration instantaneous! Any accounts required for the incident management team should be pre-registered to ensure there are no delays in staff accessing necessary systems, no assumptions should be made about individuals access to IT systems. Use of role accounts has proved invaluable to ensure that information is passed between people carrying out the same role.

2.5.1.5 Generic Action Plan

When developing a recovery plan there are two streams of action required: The first priority is to establish IT services to support critical business processes. Provision of these services will not necessarily be the long term solution e.g. email connectivity may be established in the short term through creation of temporary email accounts at another site. The long term solution is to purchase new email servers appropriately sized for all site-x users. The second stream of activity is projects to re-establish normal services.

The following generic action plan for managing an incident has been established for site-x:

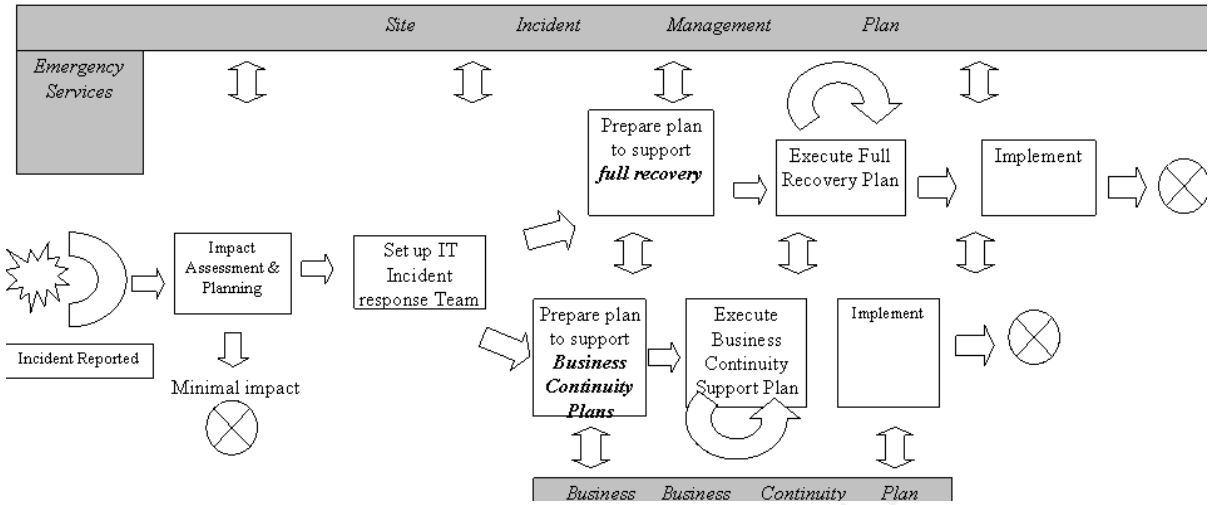


Fig 8 – Generic Action Plan

Through use of the DRP the initial meetings in preparing to support the BCPs have developed as follows:

Initial briefing meeting

The Incident team, representatives from each of the supply teams and BITMs are invited to attend an initial briefing. The briefing covers a description of the incident, an initial assessment of services impacted and critical business activity. The actions from this meeting include

- BITMs establish the critical business processes and IT services required to support them
- Support teams establish the full list of services impacted and explore options for continuity, including developing an understanding of the resources (people and hardware) required to deliver options and availability of the resources.
- Development of a communications plan. Outlines all groups that need to be contacted (site users, business management, helpdesks, other sites, IT management)

Support team meeting – 1-1.5 hrs after initial meeting

Support teams report back to IRM and Operations Rep on the full extent of the impacted services, how long it is estimated they will be unavailable, what continuity options there are and the availability of resources to implement the proposed options.

Business priorities meeting – 1.5-2 hrs after initial meeting

IRM gives update on the status of the incident and possible continuity options. The BITMs or representatives report the critical activity within the businesses. The BITMs prioritise the recovery requirements across the businesses.

The actions from this meeting include

- Support teams start to deliver IT services prioritised by BITMs and approved by the IRM

2.5.1.6 Reference Documentation

The reference documentation required to support the DRP includes

- Build information for the IT systems (inventories, dependencies)
- Business continuity information
- Contact lists (IT team, business representatives, IT management, external suppliers)
- Continuity options (suggestions on how continuity could be provided for systems where formal IT continuity options do not exist)
- Checklists for the incident team members
- Forms for the documentation that needs to be kept during an incident

IT system documentation

The support teams were asked to create system documentation for all systems which they supported, and then maintain it. The documentation was created according to company standards and held in a number of locations

- Outsourcing agreements require documentation to be kept centrally on outsource company systems
- Some systems are managed by support staff who are not based in site-x
- Many systems are built using company specifications. These are managed and stored centrally

"What happens if the entire staff of IT workers are lost, as has been the case for several companies affected by the attacks?" Will employees be able to access applications and data? (Stringer)

The emphasis of the project was to ensure that we had the necessary documentation and knew where it was and how to access it. On completion of the documentation the support teams were asked

- If documentation is held on servers in site-x, the external website is to have a copy of the document placed in it with reference back to where the original is stored. The website data is to be updated monthly, at a minimum.

- If documentation is not held on a server in site-x, the external website is to contain the reference to where the document is held and how to it can be accessed. Access could be via a person at another site.

The businesses forms on IT services required for continuity

Having captured business requirements during the Business Impact Analysis, the BITMs agreed that it would be valuable to maintain this set of information for their businesses.

Initially I regularly asked the BITMs to review and update the forms, there was little appetite within the business teams to do this. With agreement from the BITMs and IT management the forms have been dropped from the plan.

With changes in the business cycles, the forms would only ever provide a starting point of IT services required to support critical processes. Without the information there is a reliance on the BITMs having a good understanding of the business processes and IT services needed to support it, and the data required to quickly restore specific datasets is less likely to be maintained making restoration of services slower.

Contact lists

Following initiation and during an incident there are numerous people who need to be kept informed of the progress. During an incident it cannot assumed that the normal methods of accessing contact information, or contacting people, will be available so developing and maintaining lists of contacts is advisable.

I collated the following lists with office number, mobile number and emails addresses. These lists are updated at least quarterly in the week preceding the DR exercise.

- BITMs – contact information for BITM and a backup representative for each of the businesses at site-x, along with the business they represent

- IT Team – contact information for the IT team, identifying people by name and role as all staff who might be part of the incident team do not have an intimate knowledge of the support organisation

- Senior IT management – an incident will need to be reported up the management tree and into the company IT organisation as interruption of services in site-x may have knock on effects at other sites.

- Technical contacts – technical staff from across the organisation who are recognised as having expertise in delivery of specific IT services whose expertise may prove valuable in responding to incidents.

- Vendor organisations – companies who may be able to supply resources either for hire or buy (man power, computing equipment etc) required to establish services either short-term or permanently.

IT Continuity Options

Very few of the IT systems in site-x are covered by formal contingency plans. The current support teams have a vast collective knowledge about how current services are delivered, and all this knowledge is not captured in documentation. The support teams were asked to consider and document options for continuity provision that could be invoked following disaster. This list has been augmented following DRP exercise where additional services or continuity options are developed.

Following a disaster all support teams may not be available and existing support teams are likely to have a better view on options how services can be re-established. Having this initial list of options has assisted the team when deciding on the continuity options during the exercises.

Checklists for the incident team members

Following an incident there is a standard set of tasks that needs to be performed, as the incident progresses the tasks start to diversify. In order to ensure that the initial tasks are carried out I created a set of checklists which summarises the role of each team members and outlines the initial task list.

Forms for the documentation that needs to be kept

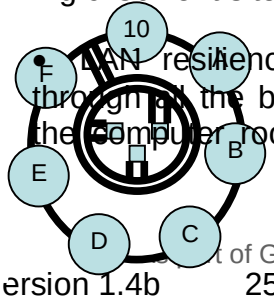
The information that needs to be documented for each incident is standard. At the start of an incident rather than having to think about how to document the incident there is a set of predetermined forms.

2.5.2 Projects to improve resiliency & improve IT continuity

In parallel with the documentation projects, the following projects had been approved to reduce some of the single points of failure. These were carried out by the support teams

- Telephone lines into site-x – the telephone lines into site-x have been split between two substations, increasing resilience of telephony.
- Telephone switches – One of the telephone switches has been moved to a different building in site-x. There is some capacity for some business lines to be moved between switches should a single switch fail.

Fig 9 Current site-x LAN topology



- LAN resiliency – A LAN ring has been created running through all the buildings in site-x, providing dual paths back to the computer rooms. Each Building and each server has dual

connections onto the LAN backbone. The single points of failure in the LAN have all been eliminated.

- WAN resiliency – A triangle of high capacity leased lines has been created between site-x and two other company sites in country. This provides additional resilience for connectivity to the rest of the company for site-x, and the sites connecting through site-x.

Two projects to improve IT continuity provision that were approved at the start of the project:

  - Email – This project was to provide email accounts for a pre-defined set of critical business users at another company site, it was estimated that approximately 10% of site user accounts would be required. A process needed to be developed to create the accounts, populate them with previous week's data from original account, and manage visibility of the accounts. We would need formal agreement from another company site to host our accounts for use during incidents, but would agree to reciprocate the service.

  - Team shared areas – A small number of teams indicated that their team areas for sharing documents were critical to their business processes. This project would provide mirroring of these critical files at another company site. The project would need to procure the necessary hardware and develop the processes to ensure only one copy is visible and editable by the users. Again we would need formal agreement from another site to host our server.

Following further pressure for the business to cut IT costs these projects to improve continuity were postponed!

2.6 Testing and Updating Plan

Through testing the incident management plan evolves. Documentation and processes that are good in theory do not necessarily work in practice, as Wallbaum acknowledges

"Software is beta tested before release. Products are prototyped and tested with focus groups before marketing. Yet too often documentation is not properly tested before final production"

Testing allows staff to become familiar with both the plan and different roles – just as it cannot be planned when a real incident will occur, equally it cannot be assumed that specific individuals will be available to form the incident management team. Whilst the best qualified people will be drafted onto the team, where an incident lasts for more than a few days there is likely to be a rota of people fulfilling the same roles. The more people who are familiar with the plan and the roles the more likely the recovery of services will be successful.

The first test I planned was a tabletop walkthrough. I developed a test scenario, a fire in the computer room. The exercise lasted approximately two hours. We talked through the meetings that we would have, discussed the interaction required with the

business and what involvement we would need from the support teams and filled in the relevant forms. The plan documents were helpful in directing the action for the team, however there was no real commitment from any of the participants to the exercise.

Subsequent tests have been simulation exercises, generally lasting all day (see 2.5.1.3 for description). The collective agreement of all participants is that the additional time required for the simulation holds real value as

- The DRP process and documentation evolves with use
- People get an opportunity to perform the roles in real-time, becoming familiar with the incident management plan, its processes and documentation.
- During every exercise we have learnt something new about the IT infrastructure in site-x or its configuration, even with documentation there is lots of information retained in peoples heads.
- Changing the scenarios allows us to develop further options for continuity provision for services that do not have formal IT continuity provision.

Since starting the test plan the DRP has evolved, recognising the lessons learnt from the tests. The significant changes as a result of plan use have been included in descriptions above.

3 After – 2004 & beyond….

The current DRP

The lack of business commitment to purchasing formal IT continuity provision does not stop the IT organisation from creating a functional DRP. There is no standard dictating the level of IT continuity provision or readiness for reestablishment of normal services that a business must have in order to have a DRP. The requirement is that the DRP is agreed by the business as meeting its requirements. The business can determine the level of risk that it is prepared to accept.

Following the DRP project, site-x has a DRP which has been proved to be functional and is up-to-date. The DRP has evolved from a theoretical plan document to a useful planning tool. The IT management team remained committed to maintaining the DRP and carrying out at least quarterly tests of the DRP.

To continue to develop the DRP the test plan needs to be expanded. To date there has little enthusiasm from either the BITMs or IT management to cause business disruption to enable us to carry out real tests. However, with the increasing effectiveness of virus attacks we have used the DRP to manage these real incidents, maybe there is a silver lining to every cloud! Through our test plan we have engaged significant numbers of the IT staff in the simulation exercises, with increasing familiarity of the plan. The expansion of the test plan needs to cover

- An incident that lasts for several days. We need to understand how the rota will work and information required on handover, and move from testing the continuity planning into further understanding how full service recovery would be developed.

- Enrolling teams from other sites to run the tests, the incident may mean that current teams are unavailable for a variety of reasons.

- Live testing to validate assumptions of impact and scope of services, however this may cause business disruption but could be the tool to convince the businesses that they need formal contingency planning!

- More formal training in the team roles, including formal incident management training to understand how to cope with outside traumas from an incident

- Expansion of the scenarios to understand interaction between different services and priorities across all service provision.

To ensure ongoing alignment of the site-X DRP with business requirements a copy of the DR strategy (copy in Appendix - B) is regularly circulated to the business leaders. The objective of this being three fold. Firstly to ensure that there is a continued understanding the IT continuity provision available, secondly to provide an audit trail of understanding of the current level of continuity provision, and thirdly to prompt a discussion about whether the current continuity provision is sufficient.

Business commitment to BCP

The business activity carried out in site-x continues to change, and IT systems supporting critical processes continues to evolve as the users expectations and systems become more sophisticated. The business appetite for developing BCPs has not changed.

Circulation of the current IT continuity provision, with realistic estimations of timescales for reestablishment of services to the business leaders has started to prompt some leaders to questioning the current IT continuity provision. Whilst they are not yet looking at their critical processes, they are starting to recognise that there are some basic IT services, email, file sharing, intranet and internet access & telephones, which like the plumbing, needs to be available for all staff without interruption.

Through the test program the IT support teams have developed a better understanding of the business critical processes and IT systems needed to support them. The BITMs have also gained insights prioritising requirements across the businesses.

IT services delivered from site-x

As a direct result of the DRP project all the IT systems in site-x have been documented. IT management have confidence that the supply teams could rebuild all IT systems in site-x. A slight modification to the change management process was

proposed to ensure that any documentation was updated as part of a change, this assists us in assuring that documentation is maintained.

The significant single points of failure for telephony and data networks have been resolved, improving the resilience of IT systems on site.

As a result of the test plan, the IT team have developed a better understanding of the complexities of the site-x infrastructure. Changes have been made to support processes for systems as a result of the exercises e.g. backup procedures have been changed. The assumption that the backup tapes could be read from second site proved invalid. The process was redesigned, subsequent testing has validated backup works across the two sites.

Risks to IT delivery

The biggest risk to IT delivery is virus attack, as demonstrated by the fact that the only live use of the plan has been to deal with this type of incident. Following use of the DRP during exercises and real virus attacks site-x has become more effective at dealing with viruses once they have penetrated the defences and got into the company systems. Site-x has developed a strategy for coping with virus attack through isolation of the site. We have identified that it is more effective to disconnect servers from the network than shut them down as 1) many viruses become effective on start-up, 2) the servers still need to be cleaned and patched, so machines will need to be turned on again 3) servers can be quickly reconnected to network where it is established that their removal causes unexpected consequences elsewhere in the company it network.

Through the DRP we are learning to deal with the results of the attacks, effort still needs to be put into stopping their effectiveness through user awareness campaigns and effective patching procedures – a topic for a paper in its own right!

The risks to delivery which are caused by single points of failure have been addressed through infrastructure projects.

The rest of the risk portfolio remains as issue, many of the risks can be mitigated through duplication of services or continuity provision. The business has elected not to do so.

IT continuity Provision

There continues to be no formal continuity provision for the IT services in site-x, the cost pressures facing the business are such they cannot yet be persuaded in the value of continuity provision. With the increasing dependence by the businesses on IT systems, to an IT professional the current level of formal IT continuity is inadequate.

As the businesses will not fund formal continuity provision, developing options for providing continuity on a best endeavours basis is the best planning we can do. Through the varied scenarios of the test plan a significant library of continuity options has been developed. Whilst there is no formal continuity available there is increasing

confidence that some services will be restored to some users within 72 hours of failure.

Owning the DRP

Since the initial DRP project completed I have continued to have ownership of the site-x IT DRP. The significant ongoing activities in plan ownership include

- Maintaining IT management commitment to importance of DRP, enabling the IT plan to remain current and a useful tool.
- Ongoing validation with business of the continuity strategy

Owning the DRP has been like a fairground ride, there are brief periods of frantic activity, when continuity planning has moved up the priority scale following for example terrorist activity, but just as quickly interest has waned as cost cutting initiatives come round, again. Continuing to maintain interest in developing a plan, with little interest from the customers in its importance can be soul destroying. A pedantic desire to complete projects helps get through the difficult times. And of course the only time when the plan will be really appreciated, is when nothing works. What does the Chinese proverb say - Be careful what you wish for?

4 References

Cole, Eric, & Fossen, Jason & Northcutt, Stephen,& Pomeranz, Hal.(2003) SANS Security Essentials with CISSSP CBK Version 2.1 Volume 1 . Sans Press. ISBN 0-9724273-6-8

Computing & Network Services, University of Toronto. “Disaster recovery planning”. http://www.utoronto.ca/security/drp.htm

Delio, Michelle. (2000) “Disaster Recovery: The Worst Case Scenario “. Availability.com.www.availability.com/news/expert_commentary/index.cfm?fuseaction=news&id=E9C80B1A-B973-11D4-868600D0B79E8E51

Hussong, William A. Jr. “So You’re The company’s New Contingency Planner!” . Disaster recovery journal. http://www.drj.com/new2dr/w3_001.htm

MessageLabs (Sept 2003) “MessageLabs' Latest Intelligence Report Shows August Was Record Month For Viruses” http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=557&region=

MCI. Instant meeting. http://e-meetings.mci.com/instantmeeting/index.php3

Palermo, David (2003). “Time to rethink your business continuity plan”. Disaster resource guide. http://www.disaster-resource.com/articles/03p_057.shtml

Rothstein, Philip Jan. (1995). “The politics of recovery testing”. Rothstein Associates Inc. www.rothstein.com/articles/politics.html

Smith, David J (ed) Business Continuity Management: Good Practice guidelines. Business Continuity Institute http://www.thebci.org/frametrial.html

Stringer, Judy. (2002) “Disaster Planners Focus on Coping with Key Personnel Loss”. Availability.com http://www.availability.com/news/expert_commentary/index.cfm?fuseaction=news&id=1053FF6B-00CB-4A28-BC5209498E9093A5

Wallbaum, Don. (1999). “Creating Usable Disaster Recovery Documentation”. Disaster Recovery Journal. http://www.drj.com/new2dr/model/w3_002.htm

Wold, Geoffrey H.& Shriver, Robert F.(1999). “Risk Analysis techniques” . Disaster Recovery Journal. www.drj.com/new2dr/w3_030.htm

Appendix - A. IT needs for Business Processes

Background

IT site-x is developing an IT response to Business Continuity Plans aimed at minimising the impact of the loss of IT Services on the business. This IT Plan covers IT services delivered in site-x for businesses situated in site-x.

An important input to the development of the IT Plan is detail on each of the business primary activities and their dependence on IT Services. This input will be used to:

- assess the impact of a loss of IT service
- prioritise the response from IT
- identify gaps in existing IT service resilience

This form is designed to gather information on business activity.

Request for Information

Business name: Prepared by: Date:

Q1 What are the business primary processes (max. 10)? Prioritise in order of importance to re-instate.

Priority	Primary Process Description	Team	No of people	Location	Periods of planned activity
example	Financial Feed	GCA	9	Bld A, Room 6	1st week each month

Example processes include - Development Planning, Commercial, Management, Acquisition & Disposal, widget manufacture

Q2 Primary Process Analysis

(Please repeat the following for each Primary Process, or groups of processes listed above).

Process:

Q2 (a) Who are the key business contacts following an incident?

Business contact name(s)	**Role**	**Contact number**	**Number type (office, mobile, home, pager)**

Q2 (b) Specify the IT Services on which the Primary Process depends.

Priority	**Service description**	**Detail**	**Function of IT Service**
1 (example)	Desktop	Email	Communication with customers

Examples of IT Services includes - Business Applications (please specify) Desktop (email, file servers), Voice (telephone & fax), Data Management,

Q2 (c) If the IT services are lost, what actions would be required to manage the loss and what would the impact be (Please repeat for each service)

(Approximate period durations can be used to specify a phased response.)

IT Service lost: **.....**	**Period 1** Duration :	**Period 2** (if applicable) Duration :	**Period 3** (if applicable) Duration :
Action/workaround e.g. do nothing, move operation to another site, manual operation			
Requirements during period			
Min. No. of personnel			
Min. No. of PC (network)			
Min. No. of PC (standalone)			
Min No. of remote access users			
Status (formal/informal)			
Impact of loss of service			

Safety (H/M/L)			
Reputation (H/M/L)			
Cost ($)			
Dependence on DATA*			
Criticality of data (H/M/L)			
Data set description			
Data set location			
Contact for data			

Include electronic and hardcopy if appropriate

Appendix - B. Strategy for IT DRP

The Office accommodation emergency plan is looking to provide accommodation for approx 500 users in different offices across the region. In support of this plan IT anticipates it would be able to provide limited connectivity using spare capacity at receiving sites. This strategy is based on best endeavours and has no pre-specified coverage for any service. Full recovery of IT services could take at least 6 months depending on the nature of the disaster.

The strategy is divided in two as follows:

Business Continuity

- There is NO hot standby facility available as this has been considered too expensive for the perceived risk
- Team created to develop short term actions to create temporary services for a small number of staff (max 10% of population) working on critical activities as identified in Business Continuity Plans (BCP)

Full Recovery

- Team created to develop program of projects set in place to deliver normal service to all staff
- Full services are likely to take 6-9 months to recreate. As services are available they would be made available to users.

Scenarios covered:

All site-x IT infrastructure destroyed.

DESKTOP & APPLICATIONS

- E-mail accounts for staff working on critical activities (approx 200) – may take up to 4 days for accounts to be created.
- NT file shares identified as critical will be restored to servers at another site where space is available at another site to restore data – may take up to a week for data to be available.

- Estimate that it will take 4-6 weeks to provide restored e-mail accounts for all staff and access to NT file shares. Estimate will take 6 months to provide full services as available before disaster.

TELEPHONES

- Personal extensions will not be available.
- Callers to switchboard can inform caller to try mobile/other numbers supplied via Global Address List (GAL)
- Estimate it will take 4-6 weeks to have a working telephone system.

Links terminating in site-x

- No continuity provision. Estimate will take 4-6 weeks for services to be re-established. As services are available they would be made available to users

Access to site-x restricted

Only staff engaged in Business critical activities should access the network via modem links

DESKTOP & APPLICATIONS

- IT Services available over modem links
- Maximum of 120 modem links available direct into site-x.

TELEPHONES

- Callers to switchboard can inform caller to try mobile/other numbers supplied via Global Address List – If access to site with switchboard not restricted

Links terminating in site-x

- Available while support staff not required

No company IT infrastructure worldwide

NO continuity provided for this scenario

Links into site-x

There is NO continuity provision for links landing in site-x if site-x infrastructure is destroyed. The sponsor of each link is responsible for defining the critically and ensuring that there is adequate continuity planning.