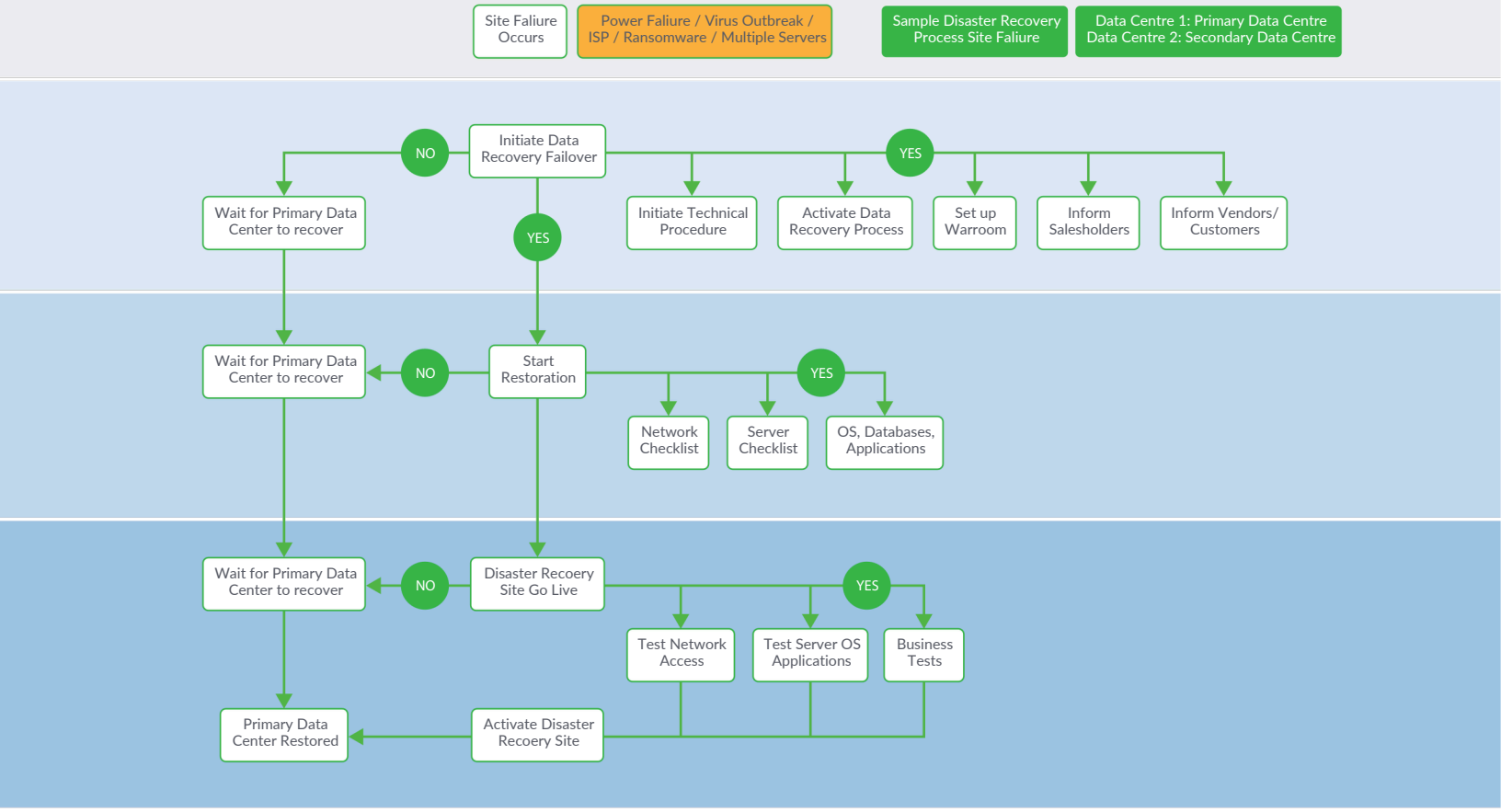

DISASTER
RECOVERY
PRIMER
Canon
Managed IT Partner
SUPRAITS
SECURING THE ESSENTIALS




Small and medium-sized organizations rely on data as the lifeblood of their business. But unlike large enterprises, you don't often have the IT infrastructure and a disaster recovery plan in place to safeguard mission-critical information.

The bad news is that it's just a matter of time before you encounter a major disruption to your IT infrastructure that results in the loss of mission-critical business data. The good news is it's easier than ever to architect enterprise-class redundancy into your business operations thanks to the cloud.

An experienced technology partner can help you develop and maintain a disaster recovery plan that anticipates a variety of scenarios that could interrupt your primary business operations. There are plenty of options available, so here's a primer as to what you should expect from your service provider.

## Why do you need a disaster recovery plan?

The purpose of a disaster recovery plan is to put procedures in place to ensure fast, successful recovery of mission critical applications and data after any disruption. It begins with a notification phase that activates the plan that alerts everyone and gets the recovery process started. The recovery phase restores temporary operations and repairs any damages that may have occurred to the original system.

A comprehensive, effective disaster recovery plan identifies all the activities, resources and procedures needed to carry out all processing requirements during interruptions to normal business operations. It also assigns responsibilities, whether it's your organization's role or your cloud service provider's.

Because there are lot of moving pieces involved in a recovery process, the plan ensures coordination and communication among everyone involved who've been assigned to the recovery planning strategy, including external points of contact and vendors.

To be truly effective, your disaster recovery plan should be guided by these objectives:

| | | |
|---|---|---|
| Minimize economic loss | Establish a solid communication matrix to be used in the event of disaster | Reduce disruptions to operations |
| Provide organizational stability | Achieve orderly recovery | Reduce legal liability |
| Limit potential exposure | Lower probability of occurrence | Reduce reliance on key personnel |
| Protect assets | Minimize decision making during disaster | Reduce delays in critical recovery situations |
| Provide a sense of security | Comply with regulatory requirements | Recover all mission critical applications within the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) |

## What does your plan cover?

Your disaster recovery plan should also be clear about what business processes are in scope, particularly if it involves your service provider:

| Business Process | Role(s) | Relevant Technical Components |
|---|---|---|
| Active Directory | | |
| All Other Services | | |
| Application Support | | |
| Backup and Disaster Recovery | | |
| Collaboration | | |
| Database Administration | | |
| DNS Services | | |
| Help Desk Services | | |
| Network Services | | |
| Security Services | | |
| Servers | | |

The scope of a typical disaster recovery plan addresses technical recovery in the event of a significant disruption. It works in conjunction with your business continuity plan (BCP) that's part of your risk mitigation strategy. A disaster recovery plan is a subset of the overall recovery process contained in the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the BCP.

**A disaster recovery plan provides:**

- Guidelines for determining plan activation
- Technical response flow and recovery strategies
- Guidelines for recovery procedures
- References to key business resumption plans and technical dependencies
- Rollback procedures that will be implemented to return to the standard operating state
- Checklists outlining considerations for escalation, incident management and plan activation

**The specific objectives of this disaster recovery plan are to:**

- Immediately mobilize a core group of leaders to assess the technical ramifications of a situation
- Set technical priorities for the recovery team during the recovery period
- Minimize the impact of the disruption to the impacted features and business groups
- Stage the restoration of operations to full processing capabilities
- Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team

## How do we know it's a disaster?

IT staff deal with glitches all the time, whether it's a trouble ticket from an end user or an alert from their application and networking monitoring tools. But at what point do you know it's time to activate your disaster recovery plan?

For the purposes of your plan, a disaster is any event that results in the specified mission critical application systems and / or data being unavailable for a period of time threatens the continued stability and/or continuance of an institution, that brings about great loss and/or damage, or that creates an inability on the organization's part to perform critical functions.

Not all incidents will trigger your recovery process, so the severity of the incident must be assessed prior to declaration. Part of developing your plan is defining those parameters. An incident is defined as any unexpected event that may or may not cause a system to function improperly.

Going a step further, a critical incident is any event that results in the impairment of business-critical functions, leaving you unable to provide essential services for a defined period. Incidents may be internal or external to business operations. For example, a production server on your premises may become unavailable, or an MPLS connection may be broken because your primary network service provider is experiencing a major outage.

## Identifying the many dependencies

The glitch you're experiencing may have wide-ranging implications. When one resource is affected, many users can be affected, and many business processes can be disrupted. Dependencies help to define whether your incident is a full-blown disaster. That's why these dependencies should be defined in your disaster recovery plan.

Here are few examples:

**User Interfaces**

End users, power users and administrators are unable to access the system through any part of the instance. This could be on the client or server side, web interface or downloaded application.

**Business Intelligence and Reporting**

The collection, logging, filtering, and delivery of reported information to applicable stakeholders is not functioning; the user interface layer may or may not be also affected.

**Storage Layer**

Loss of a storage area network (SAN) or other storage resource.

**Network Layers**

Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance.

There are many more dependencies, and your service provider is well-equipped to help you identify them so you can quickly resolve issues and take advantage of secondary infrastructure in case of an interruption that has a broad impact on your business.

### Put it on paper

As much you are a data-driven business, your disaster recovery plan is not something that should be solely digital.

Everyone involved in your disaster recovery plan should have an up-to-date, hard copy of it since a mission critical incident may make soft copies inaccessible. Both soft and hard copies should be stored at multiple locations across your organization, as well as at your service provider.

## Disaster recovery plans are living documents

Your disaster recovery plan is not set in stone. It will need to be updated as personnel change, software is updated and hardware is upgraded. Partner vendors and service providers will also change over time.

In addition, any incident is a learning opportunity to update the plan, so it's important to maintain a set of supporting documents and logs to provide reporting after the recovery process, such as problem log, timeline and executive summary. These must be kept up to date by their respective owners.

| Document | Active Participants | Review Period | Document Location |
|---|---|---|---|
| Master Plan | Name/Title/ Team | *Whenever significant changes are made in any of the following area(s): Strategy, Personnel, Hardware, Software, Links etc.<br><br>After every drill (at least twice a year)* | [Soft Copy Location Path 1]<br>[Hard Copy Location] |
| [SOP 1] | Name/Title/ Team | | [Soft Copy Location Path 1]<br>[Hard Copy Location] |
| [SOP 2] | Name/Title/ Team | | [Soft Copy Location Path 1]<br>[Hard Copy Location] |
| Disaster Recovery – Log | Name/Title/ Team | | [Soft Copy Location Path 1]<br>[Hard Copy Location] |
| Disaster Recovery – Timeline | Name/Title/ Team | | [Soft Copy Location Path 1]<br>[Hard Copy Location] |
| Disaster Recovery – Summary | Name/Title/ Team | | |

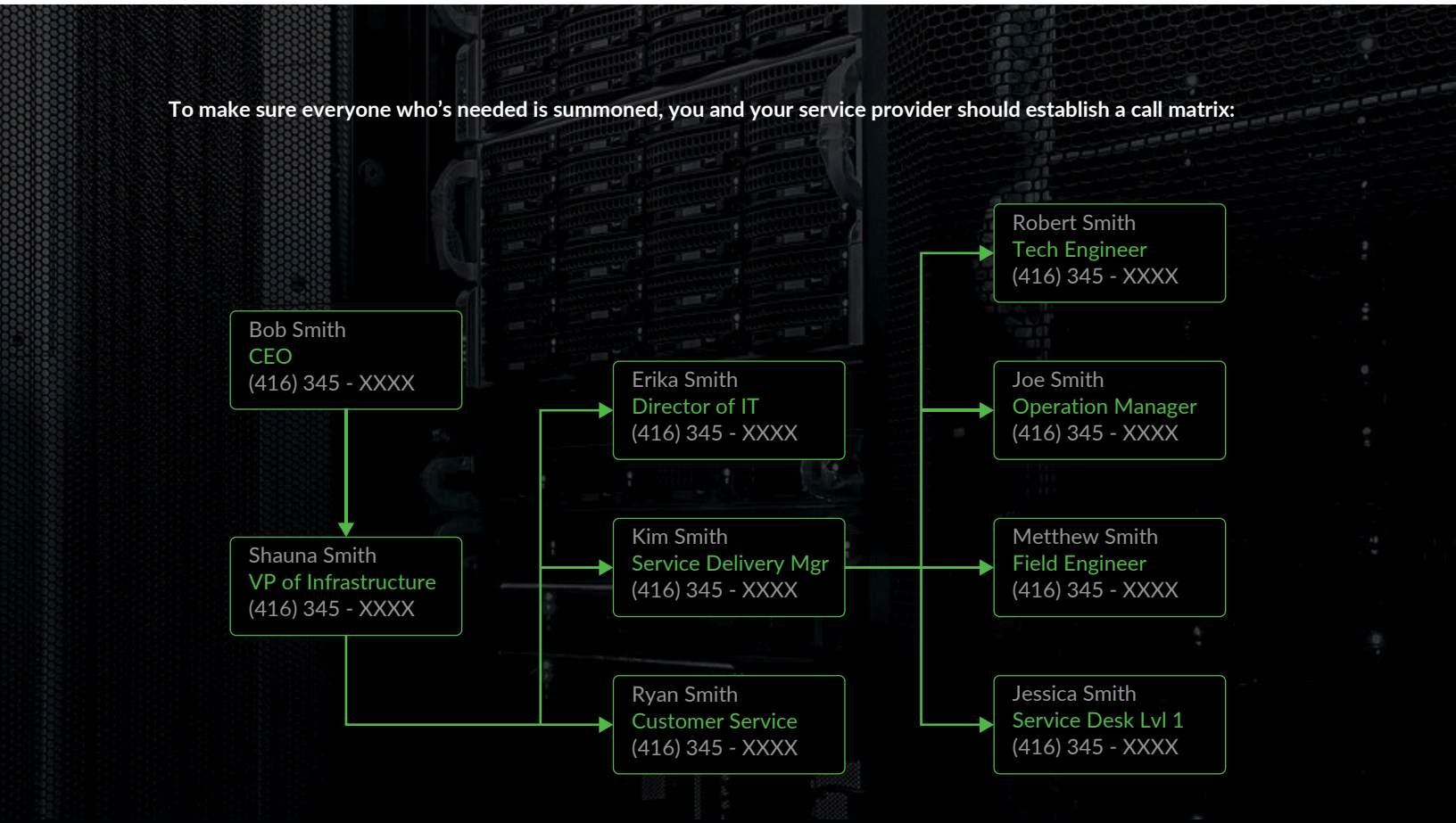
## Recovery team assemble!

Everyone in your organization will be affected by an incident that is escalated to a disaster, but there a few key people you will need if you want to bounce back quickly and minimize the disruption to business operations.

To create and maintain your disaster recovery plan, you must have a disaster recovery management team tasked with many critical responsibilities:

- Decide the incident is in fact severe enough to be declared a disaster
- Manage and coordinate the disaster recovery plan
- Authorize and activate the required teams as well as alternate facilities and secondary sites
- Review the recovery procedures to be activated that will support your recovery objectives
- Direct the team to identify the priority in which the other personnel should be alerted, whether it's those who are needed immediately or those that should remain at home on standby

**To make sure everyone who's needed is summoned, you and your service provider should establish a call matrix:**



Your disaster recovery team should include representatives from your information security group, which have specific, specialized responsibilities:

- Review the recovery goals
- Request support based on the extent of damage
- Support disaster recovery team to ensure the Information Security procedures are followed
- Assist disaster recovery crisis manager and disaster recovery coordinator with the preparation of a news media statement that outlines a description of the incident, how and when it happened, and who will be affected and now

Other team members include a disaster recovery coordinator, who can engage with your service provider and vendors so they can supply the necessary network, server, database, and storage infrastructure to support critical applications during the recovery process. The coordinator also establishes a schedule for status reports on completion of system restoration, accessibility of an alternate-processing site, and data synchronization and problem reporting.

Another critical team member is your service provider's disaster recovery crisis manager, whose priority is to keep you fully informed always and to provide a single point of contact to reach the disaster recovery teams.

They ensure all users and clients are familiar with the recovery management plan, as well as other key duties:

- Determine if any additional telephones will be required for auxiliary staffing.
- Obtain the status of operations and processing at the time of the disruption from the information security team, including general status of customer data and information, anticipated time without operating and processing services, and the availability of the next status update.
- Develop a suggested statement to be given to users, clients and media during the initial contact, and obtain approval from the disaster response management team. The statement should include a brief description of the situation, an estimate of when services will be available to users/clients, and what level of service will be provided, a request that they alert all personnel affected in their group, and assurance that users/clients will be notified in the event of any change in recovery status.
- After the disaster recovery operation is officially concluded, prepare a statement to be given to users, clients and media if necessary.

# Disaster Recovery Contacts

The contact information for all the key players in the disaster recovery process should regularly updated and easily available:

| Disaster Recovery: Crisis Manager | | | | |
|---|---|---|---|---|
| Bob Smith | CEO | (O) 416-345-XXXX Ext. 350 | (M) 416-222-XXXX<br>(H) 289-680-XXXX | (O) b.smith@company1.com<br>(P) bobbysmith@gmail.com |
| Bob Smith | VP of Infrastructure | | | |
| Erika Smith | Director of IT | | | |

| Disaster Recovery: Management Team | | | | |
|---|---|---|---|---|
| Kim Smith | Service Delivery Mgr | (O) 416-222-XXXX Ext. 266 | (M) 416-222-XXXX<br>(H) 289-680-XXXX | (O) k.smith@company1.com<br>(P) kimpossible@gmail.com |
| Ryan Smith | Customer Service | | | |
| Robert Smith | Tech Engineer | | | |

| Disaster Recovery: Coordinator | | | | |
|---|---|---|---|---|
| Joe Smith | Operations Manage | (O) 416-222-XXXX Ext. 434 | (M) 416-222-XXXX<br>(H) 905-566-XXXX | (O) j.smith@company1.com<br>(P) soccerjoe@gmail.com |
| Matthew Smith | Field Engineer | | | |
| Jessica Smith | Service Desk 1 | | | |

# Telephone Log

It's a good idea to track all outbound call attempts during the initial notification process, and for all other outbound calls.

| Telephone Log | | | | | | | |
|---|---|---|---|---|---|---|---|
| Contacted By: Bob Smith | | | | Date: April 24th, 2013 | | | Time: 03:21PM |
| Date | Time | Name | Phone Number | Reached | N/A | Busy | A) Not available<br>B) Left a message<br>C) New number given |
| April 24 | 07:30AM | Rebecca Post | 905-450-XXXX | X | | | Resolved |
| April 24 | 10:34AM | Rebecca Post | 905-450-XXXX | | | X | Not available |

## Contingency locations

A command centre will be established to direct business continuity efforts. This will be the default meeting point for all disaster recovery processes.

## The three phases of disaster recovery

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan maintained by you or your service provider, depending on the service that's disrupted.

Typically, the response phase encompasses the immediate actions following a significant event:

- Service desk is alerted
- On-call engineering team paged
- Yours and your service provider's disaster recovery team is notified and the incident is declared a disaster
- Recovery strategies are decided
- The full recovery team activated

The resumption phase covers all required activities to resume normal operations after the team has been notified; recovery procedures are implemented in coordination with any external teams to assist as need. The restoration phase is focused on tasks that will restore service to normal levels. Rollback procedures are implemented, operations restored, and monitoring is increased to ensure the full resumption of operations.

**Get back in business before your customers even notice you were gone**

The goal of a disaster recovery plan is to make sure a major disruption to your IT infrastructure has a minimal impact on your business operations.

**As an experienced technology partner with deep expertise in data protection and disaster recovery, Supra ITS not only provides secure, cloud backup services for all your mission-critical data, but helps you develop and maintain a disaster recovery plan that evolves with your business.**