

The logo consists of the text "hSo:" in a white, sans-serif font, centered within a solid black square. The background of the entire page is a solid blue color.

hSo:

# The hSo Guide to Disaster Recovery & Business Continuity

Your step-by-step guide to protecting your business

hSo:you can do what you need to do

## **Legal Disclaimer**

This free guide is designed to provide general guidance on the topic of business continuity. Whilst HighSpeed Office Limited, trading as hSo ("hSo") makes all reasonable endeavours to ensure the accuracy of the information it contains, hSo accepts no liability to you or anyone else for any action taken in reliance on this guide.

The guide is not intended as a substitute for professional advice and before making any decision or taking any action in reliance on the information contained in the guide, the appropriate professional advisor should be consulted.

## **Copyright Notice**

© Copyright 2006-2009 HighSpeed Office Limited, trading as hSo.

No content from this guide, including trademarks, may be copied without approval. Neither this guide nor materials from it may be publicly displayed or distributed for any public or commercial purpose.

## Table of Contents

Introduction.....	4
The Threats That Could Destroy Your Business.....	5
Why You Need To Prepare a DR Plan RIGHT NOW .....	6
How To Prepare Your DR Plan As Quickly As Possible .....	7
15 Secrets To Writing A Great Business Continuity Plan.....	9
Crucial Steps You Can Take To Protect Your Business .....	13
Insurance.....	13
Physical Security.....	13
IT Security.....	14
Why You Must Update Your Plan Regularly.....	16
How to Test Your Plan... WITHOUT Disrupting Your Business.....	17
How hSo Can Help You .....	18

## Introduction

A disaster can hit your business at any time. With a good DR plan, you can ensure your business survives. But writing and maintaining a good DR plan is hard.

That's why hSo has put together this simple, easy-to-follow guide to help you prepare.

**The *hSo Guide to Disaster Recovery & Business Continuity* reveals...**

- Some of the **Threats** That Could **Destroy** Your Business
- Why You **Need** to Prepare a DR plan **RIGHT NOW**
- How To **Test Your Plan** - ***Without Disrupting Your Business***
- How To **Write Your DR Plan** ... In **Record Time**
- Dozens of steps you can take **immediately** to **reduce your risks**

Everyone knows they should prepare for emergencies... but most firms never get round to it... until it's too late.

Our step-by-step guide will help you develop your own solid Business Continuity Plan. One that ensures the next disaster to hit your company isn't its last.

The fate of your business is too important to be left to chance. Don't wait until disaster strikes - start preparing today.

## The Threats That Could Damage or Destroy Your Business

- Fire
- Theft
- Fraud
- Flood
- Terrorist Attack
- Bird Flu / Flu Pandemics
- Loss of Water Supply
- Heat wave / Cold wave
- Severe Snowstorms
- Chemical Spillage
- Medical Emergencies
- Action by disgruntled/former employees
- Gas/Electricity Price Hikes
- Raw Material Price Hikes
- Supply Discontinuation
- Motorway/Road Closures
- Events such as explosions at near-by facility
- Earthquakes / Hurricanes / Landslides / Dam Breaches / Riots (if you have offices abroad)
- Hardware Failure
- Software worms
- Software viruses
- Malware
- Network Outages
- Hacker Attacks
- Electricity Outages
- Phone service Outages
- Internet Connectivity Outage
- Human error (e.g. by an IT administrator)
- Physical Security Threats (e.g. from upset customers/ex-employees)
- Strikes
- Credit Risk
- Political Risk
- Intellectual Property Theft
- Legal Risk

You don't even need to be directly hit by these threats for them to hurt you. Your customers and suppliers could be hit, with devastating effects on your business:

- Customers hit by a disaster may not be able to pay their bills, or may cease operations either permanently or temporarily.
- Suppliers hit by the disaster may not be able to supply the services you rely upon to provide your services.
- The Government may impose restrictions following floods, terrorist attacks, bird flu outbreaks, or accidents on roads/motorways that you rely upon. These restrictions may impede your business' ability to operate as usual.

## **Why You Need To Prepare a DR Plan RIGHT NOW**

If your business is not adequately prepared for a disaster, you may risk:

- endangering your staff's safety
- leaving customers in the lurch
- driving customers into the open arms of competitors
- damaging your reputation
- being sued for breach of contract or non-performance
- losing months of work
- having to pay significant sums (in mitigation costs, compensation, legal judgements, fines for breaching Health & Safety requirements)
- facing skyrocketing future insurance premiums

Your firm has insurance. But it's unlikely to cover all damages arising from all threats. It may fund the replacement of physical assets and increased cost of working. It will often cover legal costs and sometimes even lost or missed opportunities, but you'll be unlikely to recover:

- lost staff and recruitment costs
- lost productivity
- lost customers
- loss of future business to customers
- the cost of repairing damage to your organisation's reputation
- the cost of mitigating the problem
- lost work-in-progress
- late fees, penalties, Service Level Agreement payments, compensation to customers, government fines
- extra-costs from having to purchase replacements rapidly, rather than through a bid process

Disaster Recovery Planning is a sensible solution that prepares your business, so that in the event of a disaster, the interests of your shareholders, staff, and customers are protected.

## How To Prepare Your DR Plan As Quickly As Possible

In just a couple of hours, you could put together a sound plan that identifies the key risks you face and starts to safeguard your business. It won't be perfect, but it will be a good start.

### Where to start

Assemble the following information:

- An organisation chart
- Employee names, mobile phone numbers, home phone numbers, home addresses, next of kin and emergency contact details
- Copies of key contracts: building's contents insurance, medical insurance, major customer contracts, service contracts
- Key supplier contact details (including your PBX maintainer, Telecoms supplier, computer support, computer hardware suppliers and your firm's lawyers). Note your customer numbers, contract numbers and contract expiry dates. Include a diary of when all these contracts come up for renewal
- Physical Asset Inventory including equipment serial numbers, contract numbers for the purchase and maintenance agreements and details of who to contact to get the asset serviced or replaced
- Replacement Equipment Vendor account detail. You should set up an account, ready for purchasing replacement furniture and equipment in the event of a disaster
- Software Inventory, including the location of your software licenses, the registration codes, CD keys, CDs, warrantee information, and system requirements
- Customer Lists with key contact details
- The information you need to retrieve and restore any offsite data backups
- Copies of employee bank account details and national security numbers
- Employee Skills Matrix (e.g. who can fix that server? Who can arrange the payment of salaries?)
- Map showing addresses, opening hours, and phone numbers of local fire station, ambulance station, police station and local hospitals
- Details and locations of any toxic or flammable material on company premises
- Emergency equipment list (the stuff you've got to clean up the mess), and details of the equipment is kept. Typical disaster recovery equipment includes first aid kits, emergency portable lighting and a supply of drinking water
- List of staff members with First Aid training
- Map showing how to shut off the electricity, gas and water supply to your facility. It should also show how to shut off your sprinkler system
- Instructions on how to arm or disarm the intruder detection and fire detection systems. Where the firm stores portable pumps, a wet/dry vacuum, special fire extinguishers and where a central copy of all keys can be found

**What next?**

Start to identify key functional and operational dependencies to your business .

Ask each department to list its 'critical processes' in the order they need to be restored. What do they need to achieve a minimum acceptable level of service? A computer? 10 computers? What software would those computers *need*? What data would they need to access? Do they *need* email, network connectivity, phones, particular documents or particular pieces of machinery?

Discuss with management which critical business processes and services need to be restored urgently in the event of a disaster. The answer isn't 'all of them'. You need to prioritise. Once the immediate safety of your staff has been addressed, customer-facing or customer-service-affecting problems should typically be rectified first. Services supporting the entire business should then take priority over services that only affect small numbers of people.

Assemble a full set of keys and systems administrator passwords in a secure key box. That way, you'll be able to access anything that needs to be accessed, in the event of a disaster. The passwords should be secured in sealed envelopes.

# 15 Secrets To Writing A Great Business Continuity Plan

## 1. Don't Cover Everything

Remember, your aim should be to write an easy-to-follow guide, for use in an emergency. Your aim is not to write a comprehensive encyclopaedia of Disaster Recovery, to be read over several days.

Consider the actual risks to your business, then devise your DR plans accordingly. What's the likelihood of each risk materialising? What would be the impact? What would be the cost? What would it cost to reduce your exposure?

## 2. Prioritise Recovery Actions

Your plan should reflect the following:

- some tasks are more important than others to your business
- some files are more important than others
- some computer programs are more important than others
- some databases are more important than others
- some servers are more important than others, and
- some tasks can wait.

In an ideal world you would instantly return everything to normal after a disaster.

In the real world, you have to prioritise ruthlessly, concentrating your initial recovery efforts on restoring and maintaining critical business functions.

Recognise too that while many business functions are not critical in the short term, many become urgent as the length of disruption increases.

Once the health and physical safety of your staff is assured and you have saved your business assets from destruction, customer-serving activities (and the services that directly support those activities) are likely to be your top priority. Services that affect a large number of departments and staff should take priority over more localised problems.

## 3. Consult Others

You may know your company well, but the chances are that you are unaware of the full responsibilities of each department, the business-critical processes they are responsible for, and the resources they rely upon to perform their business-critical tasks.

By consulting each department, you ensure that these needs are not overlooked, and that your plan fully reflects the needs of all departments.

Once the feedback has been incorporated into your plan, test the plan on paper, with representatives from each department. This may uncover further considerations that you have overlooked. The test is also an excellent way to train the participants on the plan.

Consult your suppliers to ensure that they have adequate contingency plans in place to continue supplying the goods and services your organisation relies upon. If they do not, create your own supply contingency plans. These might include stockpiling, changing suppliers, or researching alternative suppliers for use in an emergency.

Talk to your customers, identifying those likely to be hardest hit by an interruption to your services. This will help you prioritise your recovery efforts so as to minimise customer defections after a disaster. Find out the priority each customer attaches to the various elements of your service offering, so that these can be restored in the right order.

#### **4. Assemble Information BEFORE It Is Needed In A Crisis**

If you think you don't have the time or resources to write a business continuity plan today, imagine trying to do it after your office has burned to the ground. Now's the time to prepare. In a crisis, you don't have time to waste looking for information. A disaster may destroy or make inaccessible the information you need, just when you need it most!

#### **5. Educating People About The Plan**

Make sure your staff know that your organisation has a Business Continuity plan. Ensure they know where to get a copy that is relevant to them and their department. All staff should be aware of the main points of the plan. Department heads and managers will need far more detailed knowledge.

Training is critical. If people don't know your plan exists, they won't use it. So, much of your planning will be in vain.

Remember to give a suitable copy of your plan to the building managers or security team operating in your building.

Paper copies of your plan should be available throughout your facilities and stored off-site. If your office catches fire at 3am on a Sunday, it's no good asking the guard to log on to your computer system to print out a copy!

#### **6. Document Business-Critical Processes**

Your business serves its customers by following a large number of processes. Some of these are business-critical, and yet are known to only one or two people.

It is important to document these processes, so that business can continue as usual if those key people are unavailable (due to holidays, sickness, leaving the company, or for some other reason).

By documenting business-critical processes, you will uncover dependencies, such as the requirement to have particular physical files, network connectivity, and access to particular databases. This information may help you decide which services need to be restored first.

## **7. Plan For The Worst Case And You'll Cover Many Lesser Scenarios**

Worst case scenarios deal with a total loss of assets at a given location. If you've lost your servers, only your insurer cares whether it's due to fire, flood, theft, or a stampede of psychotic bison. The recovery steps are the same for all: find a server that can act as a replacement, restore your data and ensure it's connected to your network.

By planning for the worst case, your Disaster Recovery plan will be suitable for a far broader range of events, and may therefore be kept slimmer and less complicated.

## **8. Remember Your Main Site May Be Completely Lost**

If you lose your main office or site, what will go with it? You may lose all your papers, servers, computers, telephone system, contracts, service agreements, inventory lists, paper-based accounting records, paper-based regulatory filings and tax-returns.

It's vital to back up your electronic data off-site, and to store a copy of important and irreplaceable paper documents off-site.

## **9. Don't Be a Perfectionist**

Your plan shouldn't aim to get everything back to the way it was before the disaster. It should aim to keep your business working, whilst minimising the effects of the disaster on your customers.

Recovery ought to be timely, but need not be instantaneous.

Manual workarounds are acceptable as a short-term measure.

In many cases the plan need only cover the mitigation steps needed until expert help arrives and those experts start helping your recovery effort.

## **10. Update Your Plan Regularly (At Least Every Quarter)**

There is more on this later in the guide.

## **11. Use Style and Formatting To Make Your Plan Easier To Understand**

Include photos, floor-plans, organisational diagrams, screen-dumps, numbered lists, bullet points, a table of contents and/or an index.

For example, add photos of major assets to the Asset Inventory, along with a floor-plan showing where the assets are located. If you just refer to things by model numbers, no-one will have a clue which asset you're talking about. If you asked anyone in our office to point you in the direction of the HP LaserJet 2430dtn, you would get a blank stare. It's probably the same in your office.

## **12. Remember Indirect Effects**

Many risks could harm your business indirectly. For example, fire could stop your main supplier from providing the services you rely on, or it could put your main customer out of business.

Talk to your major suppliers about their disaster recovery plans to see whether they have arrangements in place. Convey the importance you attach to them having adequate disaster-recovery plans.

Put together a list of alternative suppliers that meets your needs, so that if your main suppliers can't deliver, you've got other options at the ready.

## **13. Consider Differing Severities**

A given threat can require different levels of response based on the day of the week it strikes upon, the time of day it strikes, the location it strikes, and the extent to which there is advance warning.

## **14. Consider Opportunity Cost, Not Just Cost**

When calculating the impact of a given disaster and prioritising the allocation of resources, it is vital that you consider all costs, not just the direct cash costs. These costs may include:

- lost opportunities
- lost productivity
- lost revenue
- lost customers
- the cost of repairing damage to your organisation's reputation
- cost of mitigating the problem
- lost work-in-progress
- legal costs
- late fees, penalties, Service Level Agreement payments, compensation to customers, government fines
- clean-up costs
- extra-costs from having to purchase replacements quickly, rather than inviting competitive tenders

## **15. Ensure Each Site Has Its Own Business Continuity Plan**

Risks will vary from one site to another. The risk of flooding may be high in a lower ground office in the Thames estuary area, but of little significance to a fifth floor office in Manchester. The list of assets to be protected, the location of keys and site specific data will also vary across sites. It makes sense for each site to prepare its own disaster recovery plan, although there needs to be some strategic co-ordination to ensure consistency of standards and that company wide objectives are met. For logistical reasons, you may find it easiest to put one person at each site in charge of creating and/or updating their site's disaster recovery plan.

# Crucial Steps You Can Take To Protect Your Business

## Insurance

Disasters can be extremely expensive. If your firm isn't strongly capitalised, it may make sense to buy insurance to cover the costs resulting from fire, flood, fraud, criminal damage, and terrorist attacks. You can get cover for all of these through your insurance broker. You may also be able to get insurance to cover the increased costs you would face in mitigating the effects of a disaster.

It is vital that your company has read the wording of its insurance policies. Be aware of what's covered, what's not covered, and ensure that the coverage provided meets your company's needs.

## Physical Security

- Use **Access control** (e.g. **traditional locks** and **electronic key cards**). Approved door locks are a requirement of most insurance policies – ensure yours comply with your policy. Electronic key cards (aka 'Swipe cards') may reduce the risks of unauthorised key copying, reduce the costs of issuing and revoking keys, and eliminate the need to change locks after key loss. However in the event of a power-cut, many electronic locks will unlock, for safety reasons, leaving facilities open to physical security breaches.
- Buy **fireproof, lockable filing cabinets** for critical files. Ensure they are locked at the end of each day.
- Make sure you're protected with **Fire and Intruder Detection Systems with 24/7 monitoring**. The monitoring companies should have escalation paths to at least two trusted contact in your business, both of whom should ideally live near the facilities being monitored. Remember, fires don't just happen during the day.
- **Restrict access to sensitive areas** (e.g. to server rooms, stock rooms, financial records and regulatory records) to those who need access.
- Ensure you've got **window locks**. Approved window locks are a condition on most insurance policies – make sure yours comply with your policy.
- Get **blast-resistant glazing** or films on your glass.
- Operate a **clear-desk policy** out of hours, to ensure that intruders cannot get easy access to your confidential information.
- **Provide shredders** for the destruction of confidential printed information.
- For larger offices, it is advisable that individuals be required to wear or carry some form of **photographic ID**.
- Ensure all windows and doors are locked at the end of each day.
- Review all your information, ensuring that **all important information not available via your IT system, is copied and stored offsite**. E.g. copies of insurance contracts and customer contracts.
- **Conduct background checks** on all successful job applicants and ensure that **reference checks** form part of this process..
- **Prioritise security spending** so that if funds for security are insufficient, the most valuable assets are protected.

## IT Security

- **Backup data regularly.** Store several generations of each file. Conduct regular tests to ensure you can restore your backups.
- **Patch** all operating systems **regularly**, and patch application software as needed. Pay particular attention to the software that hackers target most, such as the operating system and the browser software. Don't forget that appliances, such as routers, may also need patching.
- Install **anti-spyware software** and update it regularly.
- Create, publicise and enforce an **IT Security Policy**. This should explain IT risks, and ban things such as the installation of unauthorised programs, the connection of unauthorised devices to the corporate network and the copying of confidential data without authorisation.
- Create, publicise and enforce an **IT Code of Conduct**. This should set standards for the use of your company's IT resources, codifying personal browsing and email rights. This will give you a basis for taking disciplinary action against those who abuse your systems. State that breaches of IT Security policy are disciplinary offences, and that serious breaches may lead to dismissal.
- **New staff** joining the business, including temporary staff, should be given an overview of your **IT Code of Conduct** and **Information Security policy**.
- Enable **Intruder-Detection** settings, ensuring that users are temporarily locked out if there are several unsuccessful attempts to log on within a short period of time.
- **Check that passwords are strong** using security utilities.
- Force all users to **change passwords regularly**.
- **Kill guest login accounts**. Every user should have their own individual accounts. Users should be made aware that they may be held personally responsible for misuse of their user accounts. The system administrators should know exactly who has access to any given information resource.
- **Change ALL default passwords, immediately.**
- Protect all servers with **Uninterruptible Power Supplies (UPSs)** that incorporate surge-protectors.
- **Test your UPSs** at least every 6 months. Ensure that they are capable of supporting servers long-enough for them to be shut down in a controlled fashion.
- Ensure **IT is immediately informed of employees that have left** and that processes exist to immediately delete their user accounts, deactivate electronic key card permissions and retrieve physical keys.
- **Lock down desktops**, so that most users do not log on as administrators, and so that only trusted users can install software without getting authorisation by the IT department.
- Ensure email is **virus-scanned** at internet level (both when being sent and received), and at each user's desktop machine. Get regular timely updates of virus definitions.
- Use at least one **firewall** per major site to protect your network. Have it configured and updated by someone who knows what they are doing. Firewalls are not a 'set and forget' technology – they need to be monitored and updated regularly. **Block access to non-standard ports**, except for those users authorised to use them for business reasons.
- If running an ecommerce site, avoid shared hosting, use **SSL** to protect credit card information, and ensure customer credit card information is securely encrypted. Alternatively use a third-party payments solution provider such as NetBanx, WorldPay or PayPal.
- Ensure that programs developed in-house perform **range-checks, type-checks and length-checks**. This also applies to web site scripts that accept inputs from the internet.

**Parse inputs to frustrate attempts at 'SQL injection'. Never trust information from Browser software.** Always check it.

- **Add 'seed names' into large prospect and customer lists.** Seed names are fake entries designed to help you catch those making unauthorised use of your data. A credible third party is paid to keep a record of the mail, phone calls or emails received by the non-existent prospect or customer. They agree to testify as to what was received. This helps ensure that if former employees start using your data at their new companies, you can find out, and takes steps to stop the misuse.
- Ensure your computers are **asset-tagged**.
- **Restrict physical access to server room, telephone switch room, vital records storage and personnel files** to staff that need such access.
- **Restrict user access** to electronic files, reports, dashboards, wallboards and database queries, so that only users that need access have it. Even when people need access to data, consider whether they need write/append/delete rights, or whether read-only access is sufficient.
- Use encryption between remote workers and your offices, e.g. use a **VPN**, and use **SSL** encryption when providing web-based access to email inboxes.
- **Document your data backup and recovery procedure**, and ensure that even if the person who normally manages your backups is away, there is someone else available who can restore your organisation's data. Regularly test that you can restore your data successfully.

## **Why You Must Update Your Plan Regularly**

You can't just write your plan and forget about it. You must revise your plan regularly, to take account of:

- staff changes
- new customers joining
- old customers leaving
- changes to customer contact details
- changes to supplier contact details
- your organisation's growth
- new insurance contracts being signed
- major contracts being signed
- new IT applications becoming critical
- changes to regulatory requirements
- changes to the law
- changes to financial audit requirements
- changes to the level of risk faced by your neighbourhood
- changes to the level of risk faced by your industry
- lessons learned from testing your plan
- lessons learned from actual disasters and negative incidents
- changes to internal processes
- changes to administrator passwords

## **How to Test Your Plan... WITHOUT Disrupting Your Business**

Testing uncovers oversights and trains your employees to handle real disasters.

### **Paper-based Testing**

Gather representatives from all departments in a meeting room and read through your plan as a group. Subject each action in your plan to scrutiny. Get feedback from everyone, ensuring you're not forgetting anything important. Those implementing your processes on a daily basis can be best placed to identify flaws or incorrect assumptions in process contingency planning.

You can run this exercise as a simulation where a pre-planned series of 'disastrous' developments occur and are introduced into the mix, as the team discuss what they would be doing.

For example, you might begin with a member of senior management being informed of a fire at your primary premises. They relay this piece of information to other members of senior management (present at the meeting) by phone. At the right point, the moderator comments that the fire brigade have stopped your access to the building. Some time later, the moderator comments that your primary premises are now entirely gutted. All the while, participants follow through on your Business Continuity Plans, saying things they would do. The moderator may note these down for later incorporation into the plan.

The easiest way to avoid disruption is to conduct the DR plan run-through on the weekend. Bribe participants with food and refreshments and/or time off in lieu.

### **Telephone Cascade**

The person at the top of the call cascade list is sent a test message, without warning, to call a designated person ASAP. They then call that number, and pass on that message to those who report to them. Each of those people should immediately phone the designated contact, who logs the time each person responded. This is a good way of checking that everyone has access to the correct contact numbers.

A disaster can happen at the weekend. So all your staff will need the home or mobile phone numbers of staff whom they need to be able to contact.

### **Full Rehearsal**

A full rehearsal is expensive. If it's conducted on a week day it can be extremely disruptive, especially if the DR plan is poorly thought out. However, if your business would be dead-in-the-water if its major premises were to be hit, it may be worth undergoing the inconvenience. Many financial firms regularly test their preparedness by swinging their IT and Communications systems over to a back-up site out of hours, and attempting to restore backup copies of their data.

## How hSo Can Help You

hSo offers a broad range of services that can help ensure your business keeps on running.

THREAT	SOLUTION
<b>Data Loss</b> due to hardware failure, server theft, water damage to hardware, worm/virus attacks, hacker attacks, human error etc	<b>hSo:VAULT</b> , our online off-site backup service, can restore your lost data, fast.
<b>Telephone Service outage</b> (circuit problem)	<b>hSo:VOICE+</b> ensures that if your primary voice circuit fails, your calls are automatically switched over to a backup circuit.
<b>Telephone Service outage</b> (main site is inaccessible) e.g. due to fire, flooding...	<b>hSo:VOICE+</b> can divert all calls to an alternative location, such a back-up site. With <b>hSo:HOMEWORKER</b> , you can divert incoming phone calls to the homes of the employees being called.
<b>Main office out of service/ Snow-Storms/ Severe Weather / Exclusion Zones in Operation/ Terrorist Activity / Bird-Flu</b>	<b>hSo:HOMEWORKER</b> lets you staff work from home, whilst being able to access their files, receive and make phone calls at the company's expense, and communicate with co-worker via phone and Instant Messaging software.
<b>Internet Service Outage</b>	<b>hSo:ACCESS</b> can provide resilient internet access. If one circuit fails, your service automatically switches over to a backup connection.
<b>Serious Server Problem</b> (Theft, Fire, Overheating, Flood, Power Outage)	<b>hSo:MANAGED HOSTING</b> puts your servers in a secure data-centre, guarded 24/7, with state-of-the-art inert-gas fire-suppression systems, multiple air-conditioning units, multiple UPS units and on-site generators .

For a limited time only, hSo is offering a **FREE 45-day trial** of our online backup service, hSo:VAULT. The trial is available to UK businesses that backup 20 Gigabytes or more.

To find out more, give us a call on 020 7847 4510.