JMS SECURE DATA

Your Data | Our Security

The ultimate guide to business continuity and disaster recovery

JMS SECURE DATA

Your Data | Our Security

The show must go on —

The ultimate guide to business continuity and disaster recovery

Contents:

JMS SECURE DATA

Your Data | Our Security

1. When disaster strikes – the facts

1 in 5 businesses face a major disruption of service every year

1 in 10 businesses that have suffered a major disaster will cease trading as a result

80% of those go out of business in 3 years

Ask yourself

- Do you have a business continuity plan?
- Do you rely solely on an insurance policy to bail you out of a disaster?
- Have you only thought as far as an emergency response or evacuation plan?
- Have you focussed solely on an IT or data recovery plan?
- Is your plan sitting on a shelf somewhere, gathering dust?

(Source: Strathclyde Emergencies Co-ordination Group, UK)

JMS SECURE DATA

Your Data | Our Security

2. Introduction: Will your business survive a disaster?

***Disaster**: Anything that disrupts a business significantly enough to cause outage and loss of revenue generation.*

Is your business disaster-proof? Disasters come in many different guises and whether they are physical threats such as a flood or fire, or something more intangible such as a hacking of your data, the effects can be devastating.

Disasters do not discriminate. Big corporations or small family-run businesses will all suffer from some kind of crisis at some point, uncovering a multitude of burning questions. What if you can't access your offices? Will your key staff members be able to work remotely? What if you lose your billing data and can't invoice your customers? Or all of your open orders? What if you lose your payroll information and can't pay your staff? These questions are not meant to alarm you but it gives you an idea of how financially and operationally crippling a disaster can be.

Businesses are increasingly virtual these days. If, for example, you plan adequate back-ups of your most crucial information, you can easily resume some of your most important administrative functions remotely. With the advancements of the cloud and internet, the ability to have an affordable disaster recovery solution hosted in the cloud is more accessible than ever before. Such solutions also enable companies to test their data recoverability quickly and easily. There are solutions that can do this without the need to utilise any disk space for testing which reduces the cost of such tests dramatically. It also speeds up testing in the already overly busy schedule of the IT professional. Some solutions have the ability to back up physical servers in such a way that the operating system can be recovered into a virtual environment immediately.

Manage unsettling times with a plan. With foresight and planning you can turn an incredibly unsettling time for your employees, customers and suppliers into one that is easily managed with a Business Continuity Plan. Whatever the size of your business, such a plan is the least expensive insurance any company can have. It details how employees will stay in touch and keep doing their jobs in the event of a disaster or emergency.

Disaster recovery of computer systems and data is a subset of Business Continuity (BC). BC covers redundancy of systems – e.g. generators in case of power outage or the ability to move to secondary premises should there be loss of infrastructure so that employees can continue their tasks down to recovering data and services. It is important to understand and establish what the basic requirements are to keep your business running should a disaster occur and have a solid, well- rehearsed plan to recover and then maintain the business in such cases

This guide will explore all the types of disasters than could happen to your business and aims to open your eyes to all the contingency plans that could be put in place – including an easy-to-follow 12-step plan at the end of the document.

3. What is a Business Continuity Plan (BCP) vs Disaster Recovery Plan (DRP)?

Business Continuity Plans are sometimes incorrectly called Disaster Recovery Plans (DRP). The two have many similarities but it's important to understand the difference:

Business Continuity Plan (BCP):

A loosely defined set of ***proactive*** planning, preparation and other associated activities to avoid and mitigate risks associated with a disruption of operations in all areas of business. There are three key areas:

1. **Resilience:** Allows critical business functions to continue despite most types of disruptions by having relevant supporting or secondary/redundant infrastructure available.
2. **Recovery:** Processes and arrangements put in place to ensure that restoration or recovery is possible for failed resilience measures. These could also be used for less critical systems.
3. **Contingency:** Ensuring a readiness and the resource capacity to deal with major disruptive or disaster type events that were both planned for and unforeseen. This is and is the last resort is the first two processes have failed for any reason

Disaster Recovery Plan (DRP):

A set of ***reactive*** procedures and policies primarily focused on the recovery of IT systems, particularly those that support business functions. Disaster Recovery is one of the many subsets of Business Continuity. Its detail would include:

- Safety and restoration of critical staff members, locations, and operational procedures after a disaster.
- Recovery strategies for IT systems, applications and data.
- This includes networks, servers, desktops, laptops, wireless devices, data and connectivity.

JMS SECURE DATA

Your Data | Our Security

4. Why should I have a BCP and a DRP?

You've worked hard to build up your business so its survival is in your hands. Or you may be a manager tasked with protecting your company's assets against any eventuality. Whatever type of business you have, your responsibilities no doubt go beyond your own financial position. You have staff to look after – livelihoods in your hands. Suppliers with contracts you must honour. You might have customers relying on you to provide a crucial service. And these days, customers expect companies to do 'business as usual' – under all circumstances.

Customers are more demanding than ever. They entrust you with their loyalty, their private data and their money – it's your responsibility to keep things going, even when disaster strikes.

So why should you have a plan? Statistics show that businesses are far more likely to survive a disaster if they have thought about it in advance, and planned accordingly.

Here are a few more reasons to consider:

Protect your future and profitability: The smaller your business, the more important it is to have a contingency plan in place. Any incident, no matter how small, is capable of impacting on your business and affecting profitability. Even if you are a sole trader, you should have a plan in place to continue your work if affected by flooding, theft or IT failures.

Guard your reputation: People are not as brand loyal as they used to be and the old adage of "a happy customer tells 1 person, an unhappy one 10 people" rings truer than ever. Customers might be sympathetic to your disaster in certain circumstances, e.g. vandalism or a force of nature, but they will remember and respect you for the way you act during such a tough time. They expect you to
prepared enough to survive.

Retain customer trust: Your customers rely on you to provide their favourite products or a crucial service. They trust you to keep their private data safe. Customer trust is earned over many years but can be broken in an instant if you don't respond correctly in the time of a crisis.

Extra insurance: It's important to check what is and isn't covered under your business insurance as that alone is not enough to safeguard your business against loss of customers and market share, or the loss of time if, for example, you were developing a new product.

Adds value: Banks, investors, insurers and suppliers take businesses with BCPs more seriously. Be sure to mention the fact that you have a BCP when applying for a loan or dealing with a new client. Efficient communication, a reliable staff and the confidence of the clients that they will be taken care of makes your company very valuable and a very attractive investment at the same time.

Builds employee confidence: A place of work is a home away from home for many employees and they expect your business to do everything in its power to protect their safety and job security. You will also need them more than ever to reassure your customers. If your employees know that they are safe, then they will inspire confidence in your clients and business partners too.

Better communication: Through your initial analysis and by regularly reviewing your plan, you will discover areas of weakness in your business which you can attend to straight away. Plus, this process, by nature, will open up the lines of communication and get departments and people communication which otherwise may not have happened.

6. Types of incidents to plan for

There are many forms of disasters and it is important for companies to have a well-rehearsed plan to recover their critical and other systems as quickly and with at least disruption as possible. Disasters could range from data corruption of a critical database, single disk or device via fault or theft up to loss of entire site.

Natural disasters:

Major incidents such as **tornadoes, hurricanes, floods, lightning striking or wildfires** tend to happen when you least expect them and no disasters are as devastating as these forces of nature. There is no 'dress rehearsal' for a flood or a hurricane. And with the onset of global warming, these incidences are becoming more common – and costly – than you may realise.

Certain parts of the world are more susceptible to natural disasters. For example, in 2012, nine of the top 10 most expensive worldwide natural disasters happened in the United States. But nothing is to say that a tsunami might not hit your city. Or an earthquake or a runaway fire.

Depending on your location, type of business or facilities there are many things to consider here but loss of utility, damage to property, safety of your crucial data and your staff are some of the most important. Natural disasters can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services.

Malicious attacks:

Vandalism, civil unrest, riots, protests, bomb threats, terrorism, robbery and reputation threats. The one thing that all of these incidences have in common is that they mean your company harm, or they put you in harm's way. Sometimes these are calculated – for example if for some reason your company falls under the spotlight of animal or human rights groups – or sometimes you literally might just be in the way (e.g. a political riot). Consider whether there would be anyone who means you harm (including disgruntled staff), or if you have offices situated in an area popular for riots, in which case think of how you would keep your staff and premises safe.

Certain attacks are not as tangible as damage to your property, such as cyber attacks – more about that further down – and reputational risks. If you have a communications department or agency, they should also be briefed on how to respond during a disaster – reassuring the public and protecting your image.

Manmade or technological events:

Systems disruptions, fires, explosions, chemical spills, communication disruption and loss of utility. Technology is a wonderful thing but our reliance on it makes businesses vulnerable to disruptions. If your line of businesses is production-based, a fire or explosion that destroys your most crucial manufacturing machine(s) could cripple your business. If you run a call centre and your phone lines go down, what then? Also the loss of power or water for an extended period could have serious consequences. What would you do if you suffered a loss of light or heat (in the case of northern hemisphere companies)? What if you can't use IT or telecoms systems or operate other key machinery or equipment?

JMS SECURE DATA

Your Data | Our Security

Cyber attacks:

Typically these kinds of attacks feature **computer viruses** (also called Trojan horses or worms) and **cyberwarfare** (cyberterrorism). Remember back in 2011 when Sony came under attack from hackers, losing almost 100 million email addresses from its Playstation database? There are many figures flying around but it is estimated that this disaster costed them around $171 million. This was spent on renewed identity theft protection, customer support, network enhancement tools, legal costs and, of course, lost revenue. All of this because a hacker felt like it.

Malicious threats could consist of inside attacks by disgruntled or malicious employees and outside attacks by non-employees just looking to harm and disrupt a business. The worst kind is that of insiders who know your passcodes and security measures. An attack can affect all components of computer security, from revealing confidential information to overloading the system's processing or storage capacity, or by causing the system to crash.

Shortages:

Until alternative **fuel supplies** become the norm, the commercial world will be reliant on fuel to continue to operate. Even if you don't operate vehicles, you will be indirectly affected by a fuel crisis. If you are reliant on transport, would you be able to operate company vehicles in the event of a fuel crisis, would your staff still be able to get to their workplace, would your suppliers be able to deliver goods to you?

Loss of workforce:

Worker strikes, disability, epidemic, outbreak of disease or infection and fatalities. They say your work force is your most important asset and at times like these, you will experience that to be true. There are many causes that could see you without your most important staff members. A seasonal or pandemic flu outbreak could seriously deplete your workforce and present serious health and safety risks. A strike over payment or working conditions will see your operations halted – and could mean physical damages too.

Human error:

Carelessness, misconduct, substance abuse and fatigue. Even if most of your operations are computerised or driven by technology, there will always be people involved. And people, as the saying goes, are only human. Sometimes they will press the wrong button, say the wrong thing, accidentally drop something on the production line or fall victim to drugs or alcohol and become unreliable.

One can be sympathetic but, in the end, mistakes can be hugely expensive and damaging for you as a company. The management of human error largely comes down to human resources – staff education, time management and so on – but you should consider how to safeguard yourself against potential disasters.

JMS SECURE DATA
Your Data | Our Security

6. Four steps to creating a Business Continuity Plan

4 steps to developing an effective business continuity plan

So now that you know the kinds of risks to consider, it's time to create a Business Continuity Plan or to revise your current plan. Your plan can be as simple or comprehensive as you desire but remember – the simpler it is, the more flexible it will be. Here are the four steps you need to follow:

1. Identify threats or risks

2. First of all, take a look at the risks that will leave your employees, customers, vendors, property and operations vulnerable. Then weight the probability of each event against its potential impact to your business, as well as your readiness to respond. Consider the following factors:

- **Historical** – what has happened in your area, to your business or operations before?
- **Geographic** – are you in a flood path, near an airport or forest, on the coast or in the city centre.
- P**hysical** – is there something about it the layout or construction of your premises that might make your business particularly susceptible to a certain event?
- **Organisational** – certain industries are particularly susceptible to certain events e.g. fatalities and strikes in the mining industry, human error in manufacturing, etc. Look closely at your employee, operational or technological infrastructure.
- **Regulatory** – this will actually help your process, i.e. is your specific business/industry required to prepare for any hazards?

2. Conduct a business impact analysis

This part of the process is about identifying the people, places, suppliers, processes and infrastructure critical to the survival of your business.

- What are your products and services? Prioritise your most crucial products and services.
- Who is involved internally and externally? Key members of staff, agencies, suppliers who are absolutely necessary to restore critical operations.
- Deadlines: what are your lead times and
- Identifying areas of potential revenue loss and listing any additional expenses that might be Incurred.

At the end of this process you should have a list of items, prioritised by need to restore each after the event. It's all about what has to be restored straight away and what can wait a week, month or a few months.

3. Develop your strategy/plan

Now you are getting to the nitty-gritty of your plan. It will list contact numbers, resources and procedures. This 'how-to' should include step-by-step instructions on what to do, who should do it and how. List each responsibility and write down the name of the person assigned to it.

Then keep all the information together in a ring binder, make plenty of copies and give one to each of your key members of staff. Also keep copies off-site e.g. at home.

4. Test, exercise and improve your plan routinely

A BCP is ever-evolving and should adapt to your company's ever-changing needs. Test and update it regularly – at least annually – or whenever critical functions, facilities, suppliers or staff change. It's important that your staff understand their roles in the execution of the plan. Exercises can include discussions or hypothetical walk-throughs of scenarios to live drills or simulations. The key is to ensure the plan works as intended. Remember to inform your insurance company that things have changed.

JMS SECURE DATA

Your Data | Our Security

7. Combat data loss – how to be prepared

A study by Kroll Ontrack reveals that 65% of companies experience frequent data loss from virtual environments. As more companies transition to cloud-based solutions, without the proper precautions, this problem will become increasingly common.

What causes data loss? Any of the following occurrences:

- File system corruption
- Deleted virtual machines
- Internal virtual disk corruption
- Storage/server hardware failures and deleted or corrupt files

The only way to safeguard yourself against these disasters is through proper data backup. This way you can minimise the disruption of your workflow and avoid losing key data. Include these three types of measures in your Business Continuity or Disaster Recovery Plan: preventative, detective and corrective.

- Preventative measures are there to mitigate or prevent an event from happening – basically to ensure that you are never in a disastrous situation. Obviously this means backing data up in the first place but not only onsite, also off site. Then also look at using generators and surge protectors, and doing routine inspections of your systems set-up.

- Detective measures are there to detect or uncover unwanted events, for example a fire, computer viruses or to protect yourself against human error. These measures include fire alarms, installing and regularly checking your antivirus software and hosting employee training sessions.

- Corrective measures focus on fixing or restoring systems after a disaster. Steps 1 and 2 you might already have in place but this final step is the most critical part of your continuity or disaster recovery plan. Here you will look at that Corrective measures may include keeping critical documents in your DRP or securing proper insurance policies.

If your company works with an outside vendor for its IT backup, ask the following questions before surrendering all physical access to files:

- Who exactly is managing my data?
- How is my data backed up?
- What happens if you lose my data?

8. How JMS Secure Data can help you

JMS Secure Data & our partners Risc IT Solutions have been providing end to end Cloud based Solutions & Services since 1999, assisting companies to protect one of their most valuable assets: their data. It is a member of the Cloud Industry Forum, EuroCloud, operates a Quality Management Systems which complies with ISO 9001:2008, and holds the Investors in People accreditation.

Our partners, Risc IT Solutions has 250 transacting Channel Partners and works with 2000 SME Customers across the UK. Its portfolio of Cloud Solutions including backup & restore, disaster recovery, virtual machines and Office 365 allows businesses to take control of costs, capacity, efficiency and productivity in order to
support them to achieve their goals regardless of size, location and business type.

All Solutions are supported by JMS Secure Data dedicated UK Technical Services & Support Team.
www.jms-securedata.co.uk/node/40

JMS Secure Data is proud to work with Attix5, who focus on the provision of secure, robust technologies that power services to increase customer satisfaction and
reduce management. Attix5
software currently operates on thousands of sites all over the world.
Their solutions are rapidly scalable, allowing them to grow with any business.