BACK-UP & RECOVERY

THE DATA RECOVERY WORKBOOK

Exercises, best practice and step-by-step guidelines for safeguarding your mission-critical data

IRON MOUNTAIN®

THE BEST TIME TO PREPARE FOR THE WORST IS BEFORE IT HAPPENS

No one wants to dwell on everything that can go wrong in business. But one thing's for sure, focusing on it after the event is simply too late.

A major loss of data can have a fatal effect on an unprepared business. Research by the London Chamber of Commerce has found that 90% of companies who suffer a significant data loss go out of business within two years. So it pays to be prepared.

Of course, not all disasters result in big, long-term problems. Something as simple as a lost laptop or a deleted file can impact at least a part of your business for a time.

THE BEST TIME TO PREPARE FOR THE WORST IS BEFORE IT HAPPENS

WHAT'S IN THIS WORKBOOK? WHAT ISN'T?

In this workbook, we'll take you through the basics of developing a plan that will help you protect your data should the worst (or not-quite-worst) happen.

We will not cover disaster recovery in its widest sense – protecting your physical locations, having alternate facilities, ensuring user recovery etc. That is a full book in its own right.

LESS THEORY, MORE PRACTICE

The focus is on practical tools and exercises (for more on why disaster recovery is so important, download our free ebook: Aftermath – Five critical lessons in disaster recovery).

In this workbook, we'll take you through five key steps to protecting your business data:

1. Getting management on board
2. Assessing the risks to your business
3. Carrying out a data loss impact analysis
4. Building a data recovery plan
5. Testing that plan

Let's get started.

1

GET MANAGEMENT ON BOARD

Everyone knows that bad stuff happens. Most of the time it is pretty minor. But every now and then it is a very big deal.

The experience of other companies clearly demonstrates that having a robust plan in place will protect your business. Aberdeen Group research shows that, when it comes to data protection, best-in-class companies recover 6.5 times faster and will likely lose 40 times less in monetary terms as a result of disruptions.

IN THE FLOODS THAT AFFECTED THE UK IN 2007, THE AVERAGE COST TO THE 7,000+ AFFECTED BUSINESSES WAS BETWEEN £75,000 AND £112,000. (SOURCE: ENVIRONMENT AGENCY.)

However, establishing an effective plan will take time and cost money. To some minor extent, it may also change how the business operates. So you will need to get management on board and committed to the process. The best way to do this is to clearly show the costs of inaction (before going to the time and expense of more detailed planning).

To determine the financial impact of various disaster scenarios (see the Aftermath ebook for details and examples) complete the following:

Yearly revenue: ..... divided by number of employees: .....

= ..... divided by 52 = ... divided by 40 = ...

This is **your hourly cost of disruption per staff member.**

Now let's look at the cost of some individual scenarios.

SAMPLE SCENARIO:

A company server storing your customer database goes down and needs rebuilding

Hourly cost of disruption: eg £192 (222Đ)

multiplied by the number of people affected: 500 = 96,000 (111,000)

multiplied by their percentage drop in productivity:
10% = £9,600 (11,100Đ) (cost per hour of disruption to your business)

1

GET MANAGEMENT ON BOARD

Over to you – copy and complete the following to assess the costs of different scenarios for your business.

With these figures in place, you should be able to show your management some indicative costs across a range of potential disasters. From here, you can have a rational conversation about what is an appropriate level of budget to put against mitigating the effects.

SCENARIO: .....

Hourly cost of disruption: .....

multiplied by the number of people affected: ..... = ...

multiplied by their percentage drop in productivity: .....

= ..... (cost per hour of disruption to your business)

2

ASSESSING YOUR RISKS

Step two is about clearly identifying what we're up against. In the Aftermath ebook we suggest that you go through a scenario planning exercise that imagines anything and everything that may affect your business' access to its systems and data.

It can be helpful to group these threats into categories. You can then look at how each may affect your business and what you need to do to protect your key data.

The following page has a useful set of questions to help you assess the possible impact of different categories of disaster. You can, of course, create your own but at a minimum you should consider:

- Environmental (eg flood, fire, storms and other 'acts of God')
- Human error (eg accidently deleting data, damaging equipment, changing permissions)
- On the move (eg lost devices, stolen laptops, back-up tapes damaged in transit)
- IT/power disasters (eg severed cables, loss of power, industrial action)
- Legal/audit (eg regulatory demands, internal audit, the need to provide evidence in court proceedings)

NATURAL DISASTERS ARE THE SINGLE GREATEST THREAT TO DATA FOR 40% OF BUSINESSES.

2

ASSESSING YOUR RISKS

THREAT ASSESSMENT WORKSHEET: SAMPLE RESPONSE

	Type of disaster: Environmental
What could affect this location – eg fire, flood, power failures, server crashes, viruses, industrial action, civil unrest, terrorist incidents etc?	Most likely would be flood damage from the local river (800m away). Storms could bring down trees on site and structurally damage the office. Fire is possible though we have argon protection in the server room – a full office fire would mean we could not access the building however.
How could this impact the business and your data – eg loss of property/infrastructure, inaccessibility, extended loss of power etc?	It could disrupt power to the property. It could limit access. Water damage to key servers.
How severe would this disruption be?	Core servers could be damaged or have to be powered down. Access may be impossible for several days. Severe structural damage could mean we are unable to enter the building.
What proportion of staff may be affected?	70% of staff have laptops and could work remotely if required. Access to email may be compromised as it is held on site (we could switch to hosted if required). CRM is cloud-based so would be available. Finance systems are local, however, and would be unavailable.
How severely?	Most departments would lose around 50% productivity. Finance would lose up to 90%.

2

ASSESSING YOUR RISKS

THREAT ASSESSMENT WORKSHEET: SAMPLE RESPONSE

	Type of disaster: Environmental
For how long?	If flood waters entered the building, we should plan for five days' disruption.
Would our back-up data be safe?	Yes. Tape back-ups are stored at a secure facility 20km away from the main office.
How accessible would it be?	We can have back-up tapes on-site within two hours (as long as the site is accessible).
How quickly could we restore data if we needed to?	As long as we have access and power, we could begin to restore data within two-and-a-half hours from calling a disaster.

2

ASSESSING YOUR RISKS

THREAT ASSESSMENT WORKSHEET: SAMPLE RESPONSE

	Type of disaster:
What could affect this location – eg fire, flood, power failures, server crashes, viruses, industrial action, civil unrest, terrorist incidents etc?	
How could this impact the business and your data – eg loss of property/infrastructure, inaccessibility, extended loss of power etc?	
How severe would this disruption be?	
What proportion of staff may be affected?	
How severely?	

2

ASSESSING YOUR RISKS

THREAT ASSESSMENT WORKSHEET: SAMPLE RESPONSE

	Type of disaster:
For how long?	
Would our back-up data be safe?	
How accessible would it be?	
How quickly could we restore data if we needed to?	

2

HOW SSB WIND SYSTEMS GOT A BETTER VIEW

Many events can prompt a business to take a fresh look at the risks to its data. For rotor blade control system manufacturer SSB Wind Systems, it was the company's acquisition by US manufacturing and technology company Emerson Electric.

Before the acquisition, SSB had always managed its own company records. As a German company, these needed to comply with Handelsgesetzbuch – the German commercial code. However, once the business became part of a US-based multinational, it had to meet the requirements of both the group's internal audits and Sarbanes-Oxley regulations.

Ultimately, this meant taking a broader view of possible risks to the business. In doing so, they had to consider a wider range of factors including:

The presence of a local nuclear power plant

Flood risks from their sprinkler systems

Threat of fire to their buildings

Possibility of theft from the premises

As a result, SSB was able to put in place a robust set of measures that both met their obligations and protected their business.

3

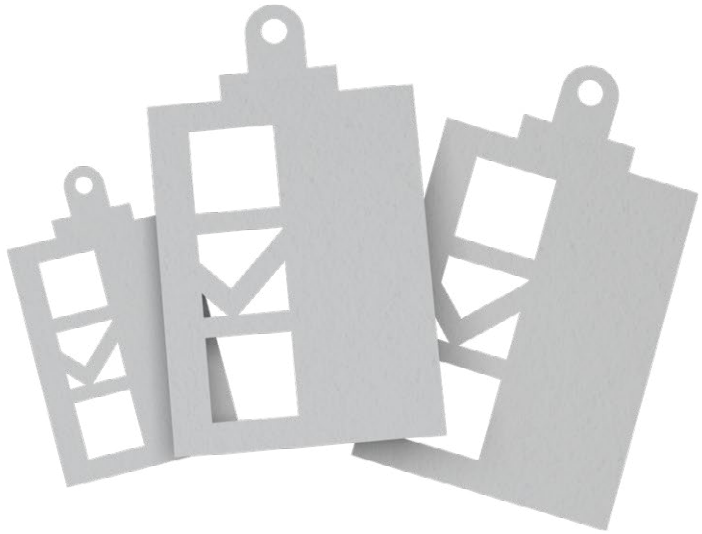
CONDUCTING A DATA LOSS IMPACT ANALYSIS

In the real world of limited funds, every company has to make decisions about what it prioritises.

When planning how to protect your data, it's important to distinguish between:

- What is absolutely critical to the survival of the business
- What is important to restore once the really critical systems are up and running
- And what can wait

Carrying out a data loss impact analysis will enable you to identify what to focus on first should a disaster hit your business. It will also help you prioritise where you invest budget to protect your data. And, when there is a problem, it will help you focus on what's important versus who's shouting the loudest.



3

CONDUCTING A DATA LOSS IMPACT ANALYSIS

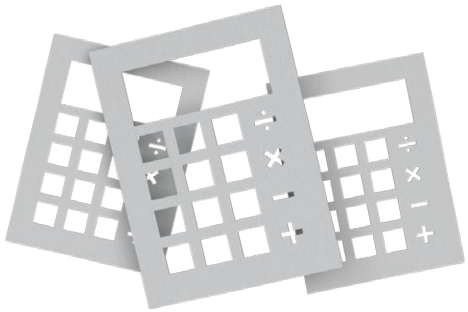
KEY QUESTIONS TO ANSWER

In any analysis, there will be specific questions you'll need to ask. Typically, for each data type, you will need to answer:

How critical it is to the survival of the business – this could be on a sliding scale (eg one to five where one is absolutely fundamental) or as classifications (eg mission-critical, important, minor).

What the loss of this data will cost the business every hour, half-day and day, both in financial and non-financial terms (this may be due to lost revenue, penalties, remediation expenses, reputation impact, compliance, ongoing backlog etc).

What resources will be needed to restore the data (eg people, expertise, equipment, facilities etc).



WHAT'S YOUR MAXIMUM ALLOWABLE DOWNTIME (MAD)?

There are some data disruptions that, if allowed to go on too long, will cause irreparable damage to your business – eg invoice and accounts data, stock control and ordering systems, ERP data. So it pays to ask a stark question: How long can any individual data loss scenario go on for before it becomes a catastrophe for the business?

The answer sets the maximum time available for recovery. Any mitigation strategies that cannot deliver within this timeframe are therefore not a viable option.

Calculating this figure is a case of escalating the costs for each system and data type on an hour-by-hour, day-by-day basis until the total amount exceeds a level which the company can bear.

3

CONDUCTING A DATA LOSS IMPACT ANALYSIS

ESTABLISHING YOUR RECOVERY TIME OBJECTIVE (RTO)

So you now have the maximum data outage time the business can survive, let's focus on setting targets for getting systems and processes up and running again. The first is to specify how quickly you plan to have disrupted data fully functional again. This is your recovery time objective (RTO) – there'll be one for each major data type.

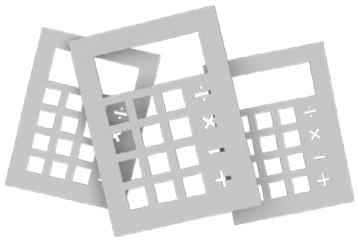
Each RTO should relate to the impact and cost of being without that data. So, a system failure that brings half the company to a total standstill and burns thousands of pounds/euros an hour needs a far lower RTO than a minor annoyance that can be easily worked around.

Of course, the cost of meeting an aggressive RTO will be significantly higher so you will need to make compromises to get to an acceptable balance.

ESTABLISHING YOUR RECOVERY POINT OBJECTIVE (RPO)

Significant disasters almost invariably involve a certain amount of lost data – typically anything that was created or amended since the last back-up (however this was performed). Your recovery point objective (RPO) will specify how much data (in time) will need to be recovered in the event of disaster-related downtime.

This has a direct impact on your back-up strategy. If you set an RTO of four hours, for example, you will need to back up the relevant data every four hours to ensure you stay within your objective. If you determine you need an effective RTO of zero, you will need to go to the expense of a fully mirrored back-up with a real-time failover capability.



3

CONDUCTING A DATA LOSS IMPACT ANALYSIS

THREAT ASSESSMENT WORKSHEET

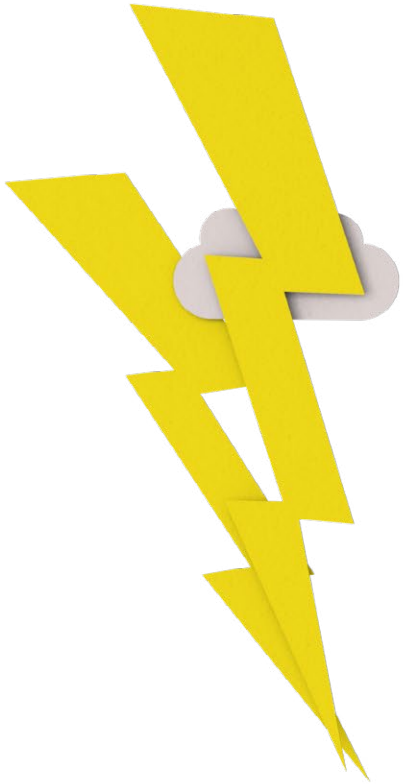
Data/system	How critical?	MAD	RTO	RPO

4

PROTECTING YOUR DATA

You should now have a clearer picture of the risks your business may face, the impact the loss of varying types of data could have, the maximum outage the business can sustain, targets for how quickly each key type of data should take to restore and the amount of data you can afford to lose.

It's now time to create a plan for how to protect your critical data.



4

PROTECTING YOUR DATA

FIRST THINGS FIRST

Using your data loss impact analysis as a guide, sort your key data types into order, starting with the ones most critical to survival.

For each, take care to identify and find all the related data as some may be hiding in less than obvious places.

Then, for each type, compare your RTO and RPO assessments with the costs of achieving them through multi-tiered back-up.

So, for mission-critical data that must be restored as quickly as possible, you may opt for a fully replicated remote site or other back-up option. For the bulk of your everyday data, you may choose professional off-site tape back-up with a timed response should you need to get hold of it. This is often faster for restoring larger quantities of data. And some data can simply be archived (again, probably to tape).

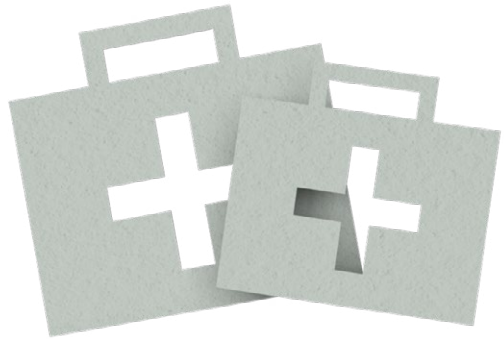
For any back-up data, you will also need to put in place a data retention policy – both to meet your RPO objectives and for regulatory purposes (you'll probably need to show this during any compliance audit).

PUT IT IN WRITING, MAKE IT KNOWN

Your data protection plan needs to be clear and easily accessible to whoever needs it. There is little point having a brilliant, comprehensive plan that sits on a server which then fails. Or one that is known to just one person who is then on holiday when a disaster strikes. And it's not just the holiday scenario. Recent research we commissioned from PwC discovered that 60% of businesses are not confident their people have access to the right tools to protect against information risks.

So when it comes to your data protection plan:

Write it down.
Print it out.
Share it.
Store it off site.



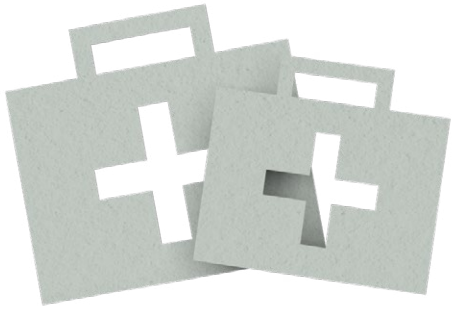
4

PROTECTING YOUR DATA

WHAT TO INCLUDE IN YOUR DATA PROTECTION PLAN

Every business is different. But there are some core elements that should appear in any data protection documentation. These include:

- How and when to invoke the plan – determining what constitutes a disaster and who can trigger the appropriate response
- Who to contact first and how to contact them
- A procedure for assessing the impact of any data loss – working through the systems identified in your data loss impact analysis
- The location of your back-up data and how to access it
- How to recover affected systems and data – focusing on the most important first
- How to declare the end of a disaster and resume normal operations



4

PROTECTING YOUR DATA

MULTI-TIERED PROTECTION – THE RIGHT BACK-UP FOR THE RIGHT DATA

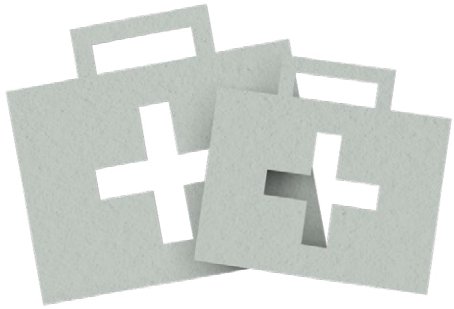
Not all data is created equal. Likewise, nor are all back-ups. For some mission-critical information, you'll want near instant access to your back-ups. For other more everyday data and archived information, there'll be an acceptable delay before you can begin restoring data.

For most businesses, having a near-instant single-tier solution – ie having all their backed up data instantly available – will be prohibitively expensive. Research by the Association for Information and Image Management (AIIM) has found that some 80% of data is never used again after 90 days. So it doesn't make sense to waste high-cost resources to make it instantly available.

Instead, the answer is to adopt a multi-tiered approach. This means mixing high-availability, high-cost options for mission-critical data (eg real-time sales data) with more cost-effective but slower alternatives for other less time-critical data (eg email, previous years' accounts, auditable information).

So for example, to meet both its regulatory and business obligations, Iron Mountain client, customer management specialist Teleperformance España must retain voice and document records for later retrieval. Different records must be kept for different periods and be retrievable within defined timescales. Some are on tape, some on CDs and DVDs, and some on paper.

We provide a weekly collection and storage service with every item having a predetermined expiry date. When a record expires, we arrange for secure disposal without any involvement required from Teleperformance España. This means the right data can be retained cost-effectively for the right amount of time.



5

TESTING THE PLAN

All plans look good in theory. It's only when they're put into action that you'll find out whether you are as prepared as you think you are. Of course, the time to spot any deficiencies is not when your servers are a metre underwater.

5

TESTING THE PLAN

DECIDING WHAT TO TEST

No plan can ever be considered complete without being tested. While you cannot anticipate every possible data scenario, you can test how well you'd cope given the most common ones:

The typical 'server down' scenario where a single server is damaged and must be restored

A power outage affecting your entire building

A flood/fire that damages a portion of your offices

A severed cable preventing access to internet, cloud and WAN services

An inability to access your building(s) due to evacuation or exclusion by emergency services

HOW OFTEN TO TEST

Things change. People come and go. New systems are deployed and old ones retired. To keep your plan up to date, you need to test and revise it on a regular basis. Ideally, you should carry out a comprehensive test every six months (or at least once per year).

Following each test, focus on what worked, what didn't and what could be amended and improved. These changes should be incorporated into the new plan and published to everyone on the data recovery team.

DIFFERENT KINDS OF TESTS

There are different levels of testing you can adopt:

Walkthrough testing – where the data recovery team talks through the steps and stages of their DR plan. This will help identify specific issues and omissions and will show whether additional training is required.

Simulations – where the data recovery team focuses on a specific scenario and runs a walkthrough of the DR plan as it would apply. This includes testing how well all the elements and participants would perform in those circumstances.

Parallel testing – where the DR team perform an actual data response using parallel equipment (ie additional systems that can be run alongside your everyday live ones).

Interruption testing – where the actual data recovery plan is invoked, back-up systems are built and the DR team performs a full cutover so that the business is running on the back-up.

WARNING: this is a high-risk test that can affect the normal running of the business. It should be approached with caution and outside normal business hours.

5

TESTING THE PLAN

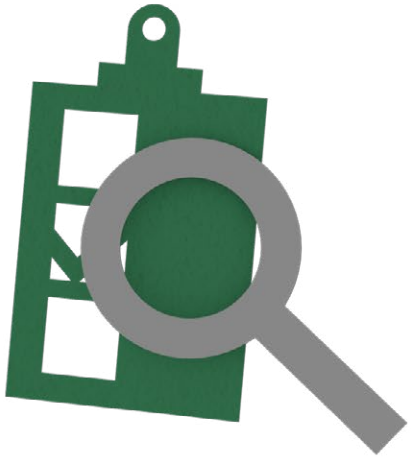
ANATOMY OF A REAL DISASTER: 07/07/2005, LONDON

Everyone hopes that real disasters never happen – especially ones on the scale of the terrorist bombings in London on 7/7. Sadly, whether it's caused deliberately by people or accidentally by freak weather conditions, these events do occur now and then.

On 7/7, Iron Mountain had 14 vehicles on the roads of the city. Roads that quickly snarled to a halt and vehicles that became un-contactable via mobile phone as the networks were suspended. While the safety of everyone involved was our top priority, we also needed to secure our clients' data.

Fortunately, all our vehicles are fitted with tracking devices. So we knew exactly where they were. This meant that when we took the decision to recall them to base, we could leave messages with their next destination using normal land-line phones.

The challenge for any disaster scenario planning is to think of the what-ifs (in this case, what if you couldn't contact your key data protection leader?). In this way, you can develop a robust plan that can deliver even under extreme circumstances.



6

BRINGING IT ALL TOGETHER

It is a sad fact of life that disasters large and small will happen over time. While you can't predict every facet of what might happen (and certainly not when it will happen), you can prepare.

Developing a realistic, robust multi-tier data protection plan is a critical component for ensuring the long term survival of your business. One that leverages both cloud and tape to get the optimum mix of availability, reliability and cost effectiveness. (Check out our Tape or Cloud? white paper for more on this.)

Achieving the right balance will help you minimise losses when disaster strikes by enabling you to bounce back as quickly as possible. It will also allow you to make informed decisions about how much to invest and where.

The recommendations in this ebook should help you get started with putting a data protection plan in place that will ensure you can recover key systems and data should the worst happen. Hopefully you'll never need to use them for a real-life disaster.

Stay safe.

7

ABOUT IRON MOUNTAIN

Iron Mountain helps organisations reduce the inefficiencies, risks and costs associated with managing their information. We can help you protect your data, streamline your business and meet your compliance requirements.

Today, we manage billions of information assets, including business records, medical data and more for organisations around the world – in every major industry and of all sizes. These include more than 95% of Fortune 1000 and over 85% of FTSE 100 companies.

We currently protect and provide access to over 65 million back-up tapes (and it's growing fast). We employ 21,000 professionals worldwide and maintain an unrivalled infrastructure that includes more than 1,000 facilities, 10 datacentres and 3,500 vehicles. With highly secure facilities, vetted personnel and an unbroken chain of custody, our standards mean your remote information is always in safe hands.

Discover how we can protect your business »