



The failures of no failover

Is your business resilient?

For any business, the loss of internet connectivity means significant disruption. It also results in significant loss of productivity and revenue that multiply every minute that you can't get online.

As our usage increases, the internet is becoming even more critical. It's not just about browsing the web. Many businesses use Voice over Internet Protocol (VoIP) to route telephone calls. You probably use some form of SaaS for project management, accounts or transactions. Many of us print and scan using internet-connected devices, cloud storage is business critical for remote staff.

A BSI survey, 36% of business owners said they feared unplanned IT or telecom outages. Those looking to gain Business Interruption Insurance need to prove they have a resilient connection to gain cheaper premiums if they are using cloud or on-line services as an internet outage can take out most of a business' critical functions.

Your internet service provider is the crucial link between your business and your future profitability. If you haven't yet audited it for resilience, or reviewed your SLAs, you should do so as a matter of urgency. This whitepaper explains how.

We'll explain:

- 1 How to ensure resilience in your internet connectivity
- 2 How to audit your provider
- 3 The options and solutions to consider when planning your resilient internet connection

Survival of the Fittest

Companies grow, in part, by achieving optimum productivity. The faster we can work, and the faster we can transact, the more opportunities we have to increase efficiency.

This is reflected in the way we sell online, the way we market our business, and the way more of our business processes are being automated.

To put it simply, we get more done in less time.

The future holds exciting possibilities: artificial intelligence, augmented reality, and virtual reality. Some of the potential commercial uses haven't yet been realised. But they all require the internet.

If your business connectivity isn't up to par, it will become more and more apparent as it falls further and further behind in this new age of technological advancement.

Productivity and “Person Hours”

If you couldn't get online for a day, what would suffer first?

- You'd probably have to send your staff home early, or ask people to work 'offline' – which is usually slower, and with the potential for duplicated work
- Your customers may become frustrated when their enquiries go unanswered, and their orders are not confirmed
- Mobile terminals may fail if they require the internet to work
- Task lists across the entire business are abandoned or delayed
- All other remote sites have to slow down to manage the decrease in throughput
- Phones stop ringing – and so do the tills

Clearly, there's a cost involved as soon as the internet goes down, and it isn't always clear exactly where the biggest costs are coming from. But we can calculate a working figure using the concept of “man hours”, or “person hours”.

One of these hours is equivalent to the work done by one person in a typical, uninterrupted hour.





Here's how it works:

$$\frac{\text{People assigned to task}}{\text{Total time to complete}} = \text{"Person hours" per task}$$

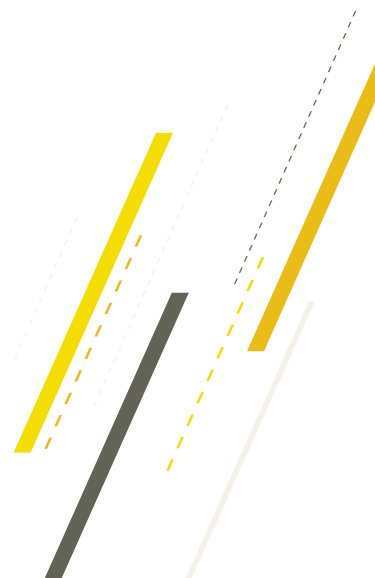
If your business uses utilisation per employee to account for revenue and profitability, being able to calculate "person hours" is key.

Only then can you measure:

- How productive your employees are in a normal day
- Where you can make improvements in process
- How much downtime it's going to cost you, if it occurs

It's important to note that this isn't a one-size-fits-all calculation. You aren't going to be able to come up with a "person hour" value across your entire business. It's more likely that you'll have a different hourly rate for each job role, grade, or department.

For example, on an IT service desk, the loss of a critical member of staff could be costly. And their "person hour" value would be different to the loss of a team leader elsewhere.



Managing the risk of an outage

If your home internet stops working, it's inconvenient, but usually won't cost you any money. An outage at work is a much more serious event, and the impact only really begins when the line is fixed:

- You'll lose productivity during the outage and catch-up period
- Some work will be done twice
- There will be clients to contact, and a backlog of orders to process
- Your customers may not be able to contact you
- Deliveries, invoicing, and deadlines will need to be managed
- If you offer an SLA, there could be financial consequences there too
- Online transactions stop!

Many businesses fail to realise the massive implications of lost connectivity, and will fail to put measures in place before the worst happens.

But these risks can be mitigated. And a little pre-planning goes a long way when it comes to internet resilience.

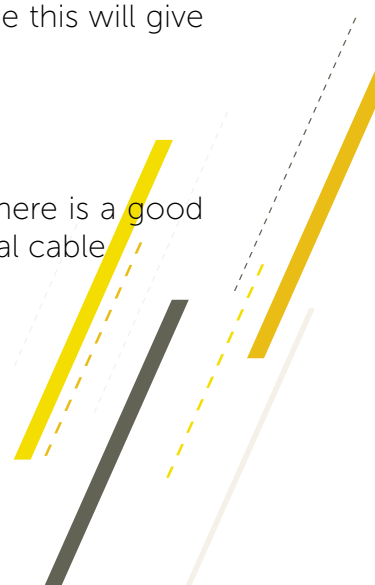
Reviewing Your Internet Resilience

You need to know that your internet service provider is resilient enough to handle the demands of your business. In order to do this, you need a few fundamentals about how your internet is provided.

Many businesses buy two circuits from two different suppliers. They assume this will give them resilience; if one goes down, the other will still function.

That isn't always the case.

Different suppliers do sometimes use the same cabling route. If they do, there is a good chance that both will fail at the same time, because a power fault or physical cable damage will likely take both out simultaneously.



So, here's your checklist when reviewing resilience today:

- 1 **What is the potential financial impact of failed connectivity?**
Consider all areas of your business. Shutting down one site could impact the others, and it could have a knock-on effect on your public relations, reputation, and brand image.
- 2 **What protection does your current internet service provider offer?**
It's very important to understand what measures are in place already.
- 3 **What do your terms and conditions say?**
Is there an SLA that will protect you?
- 4 **What kind of technical infrastructure are you reliant on?**
You might need to know:
 - Whether your services are using the same circuit, or the same exchange;
 - Whether you have a contingency plan if the primary connection fails;
 - If there is a failover from the primary connection to the secondary one, and how this works in practice;
 - Whether the two lines that you use are comparable in terms of speed.

As a result of this fact-finding exercise, you should ideally find that:

- Your business benefits from an automatic failover, without the intervention of on-site staff
- Your provider(s) offer timely and accessible support, including clear timelines for resolution of faults.

But the process doesn't stop there.

Comparing SLAs

When we talk about internet services, we often talk in terms of percentages. You'll probably see 99.95%, or 100%, when reviewing your SLA.

What's the difference?

It sounds tiny, 0.05%. In practical terms, that 0.05% equates to four hours of downtime, without penalty to your provider. That means you'd lose half a day before your internet service returns to normal, and there would be nothing you could do about it.

If you see a 99.9% SLA, it looks impressive too – but it's actually worse.

Review the SLAs from each ISP, and check exactly what's covered. Are there maintenance contracts? Is testing done? As part of this review, you should reach out to the presales team or design authority at the ISP. Ask about risks and overlaps in internet connections with the network.



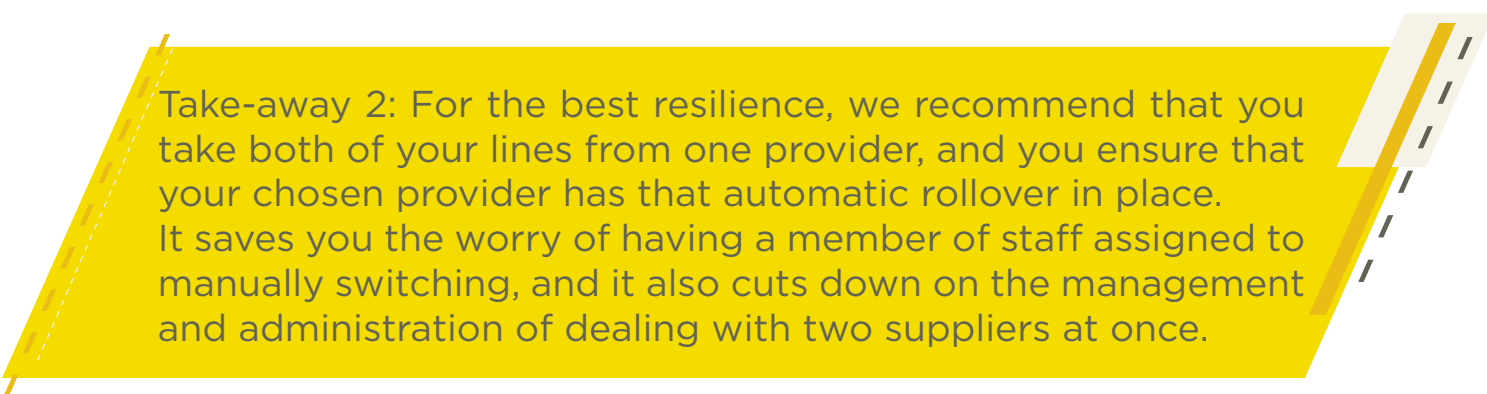
Take-away 1: When comparing SLAs, think carefully about the potential cost of four hours' downtime, or more.

Mixing and Matching ISPs

One of the common problems businesses face is the management of multiple internet service providers (ISPs) providing separate connections.

It sounds like an ideal scenario to avoid downtime, but in practice, separate ISPs rarely work well together. That's because there's no automatic failover from one to the other.

Additionally, many ISPs share the same physical infrastructure. They may buy services from each other. Almost all of them buy services from BT. There is a good chance that different ISPs use the same path, making this an ineffective strategy against resilience.



Take-away 2: For the best resilience, we recommend that you take both of your lines from one provider, and you ensure that your chosen provider has that automatic rollover in place. It saves you the worry of having a member of staff assigned to manually switching, and it also cuts down on the management and administration of dealing with two suppliers at once.

Your Internet Resilience Action Plan

The previous chapter has given you a glimpse of the common issues that businesses face when trying to achieve resilience in their internet connectivity.

Even with this quick review, we can see best practice guidelines emerging:

- Your business needs two lines to ensure that it always has a connection
- It needs to take both lines from the same ISP
- There should be an automatic failover from one to the other
- It should mix technologies and/or entrance routes so that it's protected against the common problems businesses face with wired connections

If you choose a provider that offers these things, you're well on the way to achieving 100% reliable internet connectivity.

Of course, the ISP you choose cannot cover all bases. It's worth discussing your plans with them to decide whether your internal infrastructure is ready to take on a new resilient service.

Options and Solutions

Knowing all of the available solutions will help you to achieve the best possible resilience, with the most suitable features, at the best possible price.

ADSL / FTTC / 4G backup

This is a popular choice for businesses that want a low-cost option.

This isn't a premium solution, so there are disadvantages. The bandwidth or performance criteria of the primary line will be lower than you'd get with some other solutions.

Additionally, you probably won't get an SLA, which means that there's no promise faults will be fixed in a specific amount of time.

Finally, it's very likely that the lines will come from the same exchange as the primary service; your provider may not know this, or may choose not to disclose it.

However, for a very small business that is price-sensitive, this may be the best starting point.

Two connections to the same exchange

This is an easy solution to implement; a second line runs from your premises to the exchange.

But as we've discussed, both circuits run to and from the same place. So, it's very likely they'll take the same route. And if one line suffers physical damage, there's a good chance the other will as well.

Two connections to different exchanges

This is a better solution. It gives you true resilience against physical damage or power outages at the exchange.

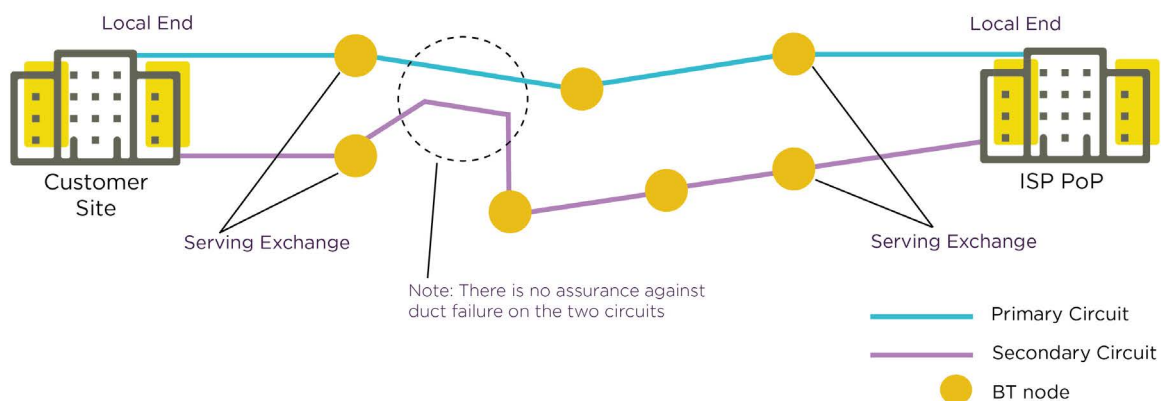
This option requires your ISP to have a skilled engineering team. You'll usually find that it's offered by ISPs using BT Openreach infrastructure.

If you choose to go down this route, there are two options:

Resilience Option 1 (RO1): A single circuit with different fibre paths between the same start and end points, available on 100Mbps services. The line has one set of Network Terminating Equipment (NTE).

The secondary service is a "hot standby" or always ready failover, with a 50-millisecond failover time if your primary route fails. This service assumes that both lines are the same capacity (and, therefore, the same speed).

The failover is controlled by the NTE, which is managed by BT; the risk here is that your ISP does not have direct control over the failover circuit and cannot test it.



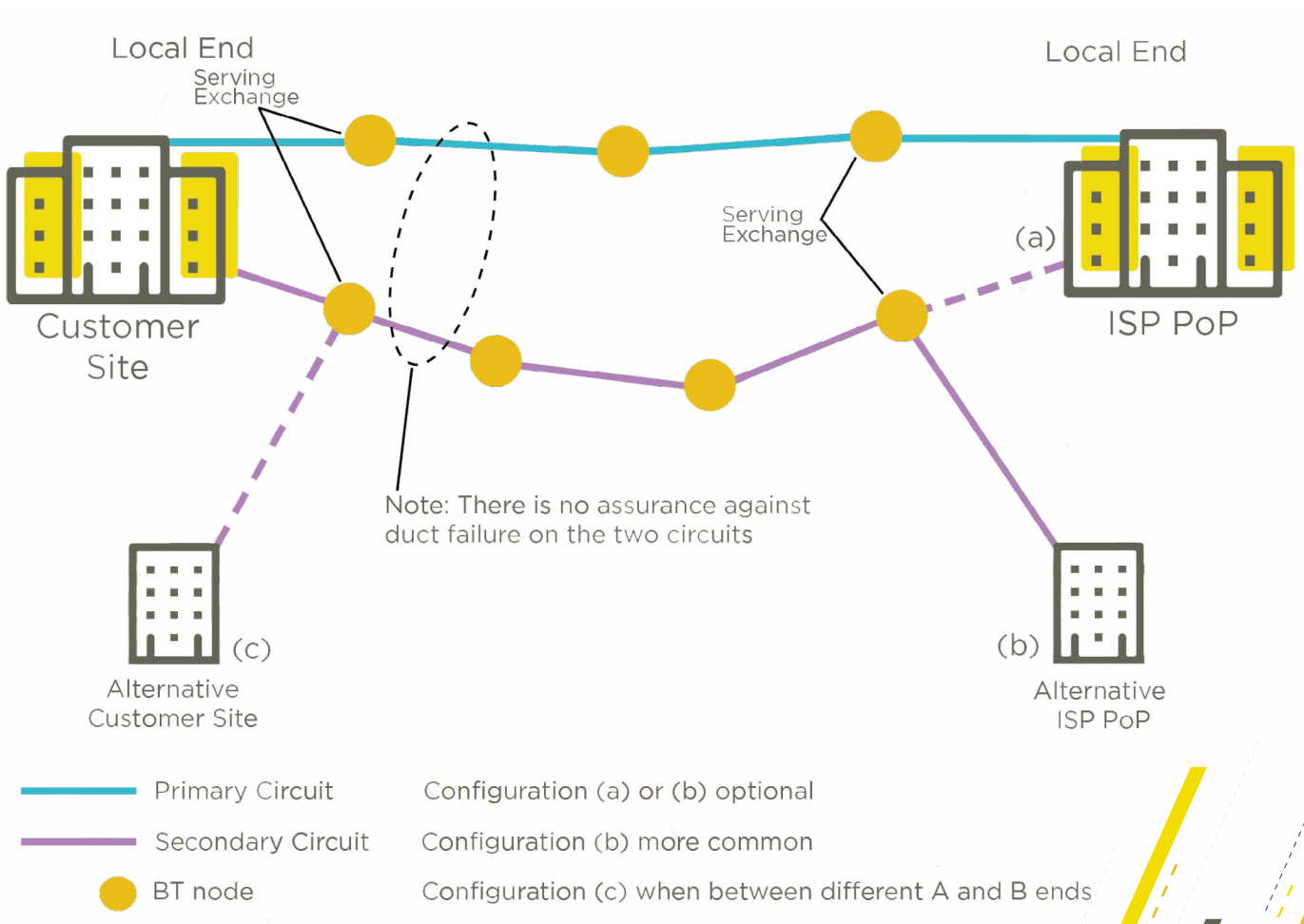
Resilience Option 2 (RO2): This is essentially two separate fibre services, so there are many ways to handle failover.

With this option, your connections may start and end in the same place, but they do not have to. You could, alternatively, have the same starting point and two different end points, or you could have different start and end points for each one.

Terminating the connection in different locations allows your ISP to use separate core network nodes thereby increasing resilience.

Your business could also have the two lines entering the premises in different places. If you can't have the lines entering in different places, you could pay an excess construction charge (ECC) which is added to the installation fee.

You'd also benefit from separate NTEs, and the failover is typically provided by the CPE – the consumer-provided equipment. This gives your ISP much more control and visibility, because each connection can be monitored and tested independently.



If you're considering RO2, it's important to obtain a technical document to assist with the design. Every ISP is different, and every in-house IT resource is different. It's important to get advice from engineers.

Finally, be sure to enquire about the specific wording in your contract. When discussing resilience, ISPs sometimes say that common ducts and cables are avoided "wherever possible"; this does not guarantee that your service has no common points.

Different technologies: fibre and wireless

This option has some common characteristics with RO2. By mixing different paths, resilience is baked into the design of your solution.

With this configuration, the fibre connection runs underground, and the wireless connection runs over the air; it is sometimes referred to as "radio", or "wireless radio". Typically, it will be received from the roof, while the fibre connection runs from the ground, and where possible, there is no overlap between them.

The last two-mile paths take different routes, so this protects against the risk of severed cables or damage to underground infrastructure in the local area.

Wireless radio circuits can be installed on separate NTE and CPE equipment, and – like the RO2 solution – your ISP can monitor them independently. Both come with an SLA and assured times to fix.

It's important to remember that these two lines will be provisioned from different exchanges, so consulting with your ISP's pre-sales authority is essential to get the best design.

Wireless radio services can be mixed with single fibre services, or resilient fibre services.

Purchasing from Multiple Providers

We've already looked at the resiliency risk of mixing different providers.

The most important thing to consider is the potential for them to share the same physical infrastructure. In some cases, they may purchase services from each other, and cannot be considered truly separate – at least for the purposes of designing a resilient connection.

There's no guarantee that multiple providers will not use the same path or ducting, for example. And they may even be provided by the same company over the last mile.

If you still want to go down the route of purchasing from multiple suppliers, ask them:

- Whether the provider has purchased the service from another provider, and if so, who that provider is
- What duct route the connection takes
- Which exchange the connection is terminated at
- Whether the connection interconnects with the provider's network

You may find it difficult to get clear answers during a risk assessment, and you will probably find it difficult to achieve true resilience. Although it sounds illogical, buying everything in one place is often more transparent, because the provider you choose is more likely to be able to tell you exactly where the common points are in the design.





In Summary

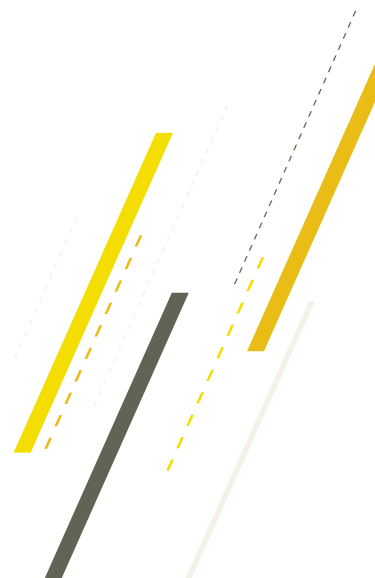
It's critical that you review your internet resilience before an outage occurs. If you don't, you could find your business losing money and customers completely without warning, and you'll be powerless to do anything about it.

The financial implications – in lost transactional revenue, productivity, penalties, lost customers, and brand damage – can be enormous, and very difficult to recover from.

Achieving resilience can be costly, but there are options for businesses of all sizes. The key is to go into the procurement process with full sight of the risks.

Our advice? Find a good partner. Ask them the right questions; uncover the detail. Work with a company that is transparent, proactive, and clear about the risks and common points. And make good use of their technical design team.

What's your current resilience solution? You probably aren't where you need to be. Disaster planning now could save your business a lot of money and interruption in the long run.



To find out how our
technology can transform
your business get in touch.

For our Sales Team call **0800 066 2739**

For our Support Team call **0161 822 2580**

Alternatively email our friendly team at **info@m247.com**