



What Does Network Instability Cost Your Business?

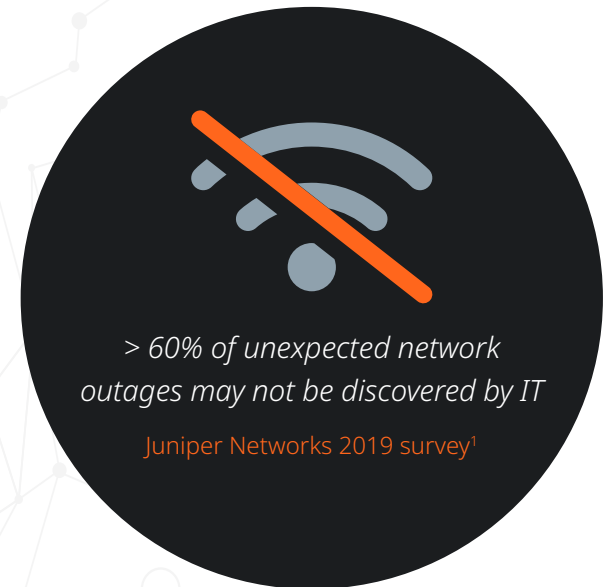
Introduction

How confident are you that your business is placing sufficient emphasis on the stability of its network? Are you prepared for the costs, financial and personal, that could result from periods of network downtime?

Evolution of businesses and their processes mean that network stability isn't just a nice-to-have. It's an integral part of day-to-day functioning and business viability. The digital transformation that enables organisations to thrive in an increasingly competitive environment needs to be supported by respecting the infrastructure at its heart. Companies that fail to prioritise the protection of their network do so at their peril.

With at least 20 major IT downtime incidents predicted to take place each year⁶, businesses experiencing outage issues are clearly not alone. But you can minimise the impact on your own organisation by taking steps that should dramatically reduce the risk of downtime disaster.

Here we consider some of the causes of network outages, what the ramifications can be, and give some practical pointers on how to improve network stability so you can keep ahead of the competition.



Contents

- 4 Causes of downtime
 - 4 Planned downtime
 - 5 Unplanned and unexpected outages
- 6 Consequences of outages
 - 6 Financial
 - 7 Staff morale
 - 7 Company reputation and competitiveness
- 8 How can outages be minimised and damage mitigated?
- 9 Four actions to reduce network instability



Causes of downtime

Networks can have performance reduced, or become completely unavailable, for a variety of reasons.

Examples of outages:

Type of outage	Planned	Unplanned	Unexpected
Reason for outage	Downtime scheduled for maintenance by the business or its service providers	Attacks, e.g. ransomware, maliciously inflicted by individuals or groups acting in bad faith	Outage due to infrastructure failure or problems due to human error

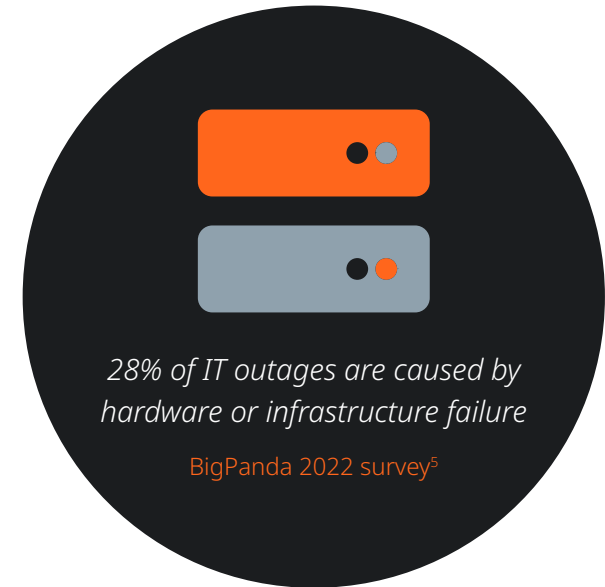
While there are many causes of IT outages, a recent survey found they often occurred because of hardware/infrastructure failure, configuration problems, or human error⁵.

And it is not just your own organisation's outages that can impact your business. Your network providers, outsourcing partners, and product/component suppliers will also schedule maintenance and can also be exposed to unexpected outages.

Planned downtime

Scheduled network outages can arise for internal reasons, such as infrastructure upgrades and maintenance. There are external factors to consider too, such as planned power cuts from electricity suppliers.

While potentially costly, when downtime is planned, contingency arrangements can be put in place ahead of time, to reduce the impact.



To mitigate winter shortages due to international conflict, the National Grid Electricity System Operator implemented a Demand Flexibility Service designed to avoid disruption. Without such measures, businesses could expect to see managed interruptions to electricity supply².

Unplanned and unexpected outages




While some outages are caused by unplanned or unexpected drops in network quality, the risk of such events occurring can be reduced through an improved network strategy.

Unplanned network outages lose revenue of \$420K per company on average

Juniper Networks 2019 survey¹






Strategic factors that may increase the risk of unexpected downtime include:

-  Routine maintenance and tech upgrades not being prioritised, which heightens the risk of infrastructure failure.
-  Complex infrastructure landscapes may not be fully understood, resulting in businesses being unaware of where their security could be breached.
-  Under-resourced IT teams may not have the capacity to deal with every potential problem so are forced to prioritise, which could lead to some weaknesses not being addressed.






Human error is a common cause of unplanned outages:

-  With workplace changes and an increased use of multiple devices, employees may inadvertently put network stability at risk when using manual practices (due to a lack of automation) combined with a high rate of change for critical projects introduces the likelihood of human error.
-  Employees may click on a link in a convincing phishing email or open an apparently innocuous attachment infected with malware, leading to a ransomware attack.
-  Staff shortages and lack of upgraded skills may lead to teams being overstretched and unprepared, increasing the likelihood of mistakes being made.



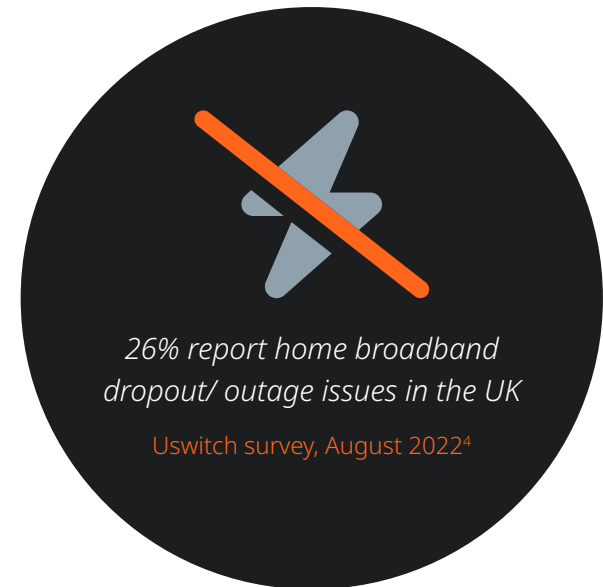
Natural and man-made disasters can also lead to lengthy downtime, including:

-  Extreme weather events such as wildfires and flooding
-  Wars, civil unrest, and targeted arson attacks
-  Lightning strikes causing regional power outages



Consequences of outages

The effects of downtime extend far beyond the duration of the outage - which the Uptime Institute reports as lasting over 24 hours for almost 30% of major public outages⁶. The fallout stretches from financial performance to public perception, and can also be demotivating for employees.



Financial

IT outages can levy a huge financial cost on a business. The exact amount will depend on several variables, such as industry sector, business processes, and number of employees. A recent estimate by BigPanda and Enterprise Management Associates reported an average cost for an IT outage of \$12,913 per minute, although for larger businesses, this rose to >\$25K per minute, or an eye-watering >\$1.5 million per hour⁵.





Depending on the nature of the business, financial costs may extend further than lost sales and productivity, into compensation to customers for failure to provide goods or services in a timely manner. A 2022 survey revealed broadband providers paid compensation to almost a quarter of the customers who complained about long outages³.

With the recent uptick in working from home and hybrid working, the extent of an organisation's network goes far beyond the confines of their traditional office spaces. Dropouts and outages are reported as the most common problems with home broadband⁴, affecting around 1 in 4 surveyed. In one year, the average home worker experienced almost two days' internet outage, which was estimated to have cost the UK economy £1.28bn³.



Staff morale

In the event of network instability, staff morale can be damaged in a number of ways:

-  The whole company has the frustration of trying to do their jobs while essential digital tools are not functioning correctly
-  Customer Services may have to deal with customers angered by the outage, which adds stress to an already challenging job
-  Infrastructure teams are under pressure to stabilise the network, while dealing with complaints from frustrated colleagues
-  Skills shortages exacerbate issues - an underskilled, understaffed IT team is unlikely to provide the quick solutions colleagues need

Unless instability problems are resolved in the longer term, staff morale will be poor, and talent lost to competitors.

Company reputation and competitiveness

Even relatively short-lived disruption to services can affect customer loyalty, losing the company sales and damaging metrics such as Net Promoter Score.

Having to solve the issues resulting from network instability will also incur an additional cost to your business, by diverting a busy IT team. It forces them to be reactive and fix the existing system, rather than being proactive and innovating your network. Unless this vicious circle is broken, progress will be impeded, and competitiveness reduced.



How can outages be minimised and damage mitigated?

Having a business continuity strategy in place to keep things running, even when unforeseen problems arise, can help minimise issues. It is perhaps no surprise that the companies who perform better are those who deal with outage problems faster¹.

With over a quarter of outages caused by infrastructure and hardware failure⁵, making sure infrastructure is up-to-date and subject to a routine maintenance schedule is a vital part of a successful network strategy.

In addition, it's important to scrutinise the network strategies of all your stakeholders, to minimise the risks of their outages to your business.

A dark circular graphic with a clock icon at the top. Below the icon is a text box with the following text:

Top-performing companies solve > 1/2 problems in < 4 hours, when others only fix 1/6.

Juniper Networks 2019 survey¹

Four actions to reduce network instability

Here are four key steps you can take today to improve the stability of your network:



1. Review your network redundancy capability

Put backup pathways in place to ensure that failure of part of your network doesn't destabilise the whole system. Routinely test network failover to ensure that business services continue to operate as expected during reduced resilience.



2. Keep security up to date

Ensure all software versions patches and updates are actioned promptly, to minimise the risk from known security vulnerabilities. Manage and update support contracts, and remove/replace out of date hardware.



3. Use modern monitoring tools

Visibility of your whole system and critical business applications enables known risks to be minimised proactively, and breaches that do occur to be dealt with swiftly.



4. Educate employees about their role in network stability

Employees may be unaware that they could personally put network stability at risk. Put a clear process in place for management of applications on employee devices, give employees access to prompt help desk advice, and make sure they have a simple way to report accidental breaches.



BESTPATH

We're BestPath. The unsung heroes, working quietly and competently behind the scenes to inspire and empower our clients. Combining curiosity with innovation we deliver agile, secure and trusted network infrastructures that enable businesses to deliver exceptional services and outstanding customer experiences. Let's chat about how we can do just that, for you.

To learn how BestPath can help you identify and manage your network vulnerabilities to avoid costly outages, contact us today info@bestpath.io



[linkedin.com/company/bestpath/](https://www.linkedin.com/company/bestpath/)



info@bestpath.io



+44 (0)203 879 4826



References

¹Juniper Networks. **Understanding Network Brownouts. Five Steps to Discover and Manage Network Slowdowns.**

<https://www.juniper.net/content/dam/www/assets/white-papers/us/en/understanding-network-brownouts.pdf>

²National Grid ESO (2022). **Winter Outlook Report. Helping to inform the electricity industry and prepare for the winter ahead. Published 6 October 2022.**

<https://www.nationalgrideso.com/document/268346/download>

³O'Halloran, Joe (2022). **Brits battered by broadband outages in past year cost UK economy £1.3bn. Computer Weekly, 29 June 2022.**

<https://www.computerweekly.com/news/252522155/Brits-battered-by-broadband-outages-in-past-year-cost-UK-economy-13bn>

⁴Uswitch. **Broadband statistics, accessed 25 January 2023.**

<https://www.uswitch.com/broadband/broadband-statistics/>

⁵BigPanda (2022). **BigPanda Report Finds IT Outages Cost Businesses \$12,913 Per Minute on Average. 01 November 2022.**

<https://www.bigpanda.io/press-release/bigpanda-report-finds-it-outages-cost-businesses-12913-per-minute-on-average/>