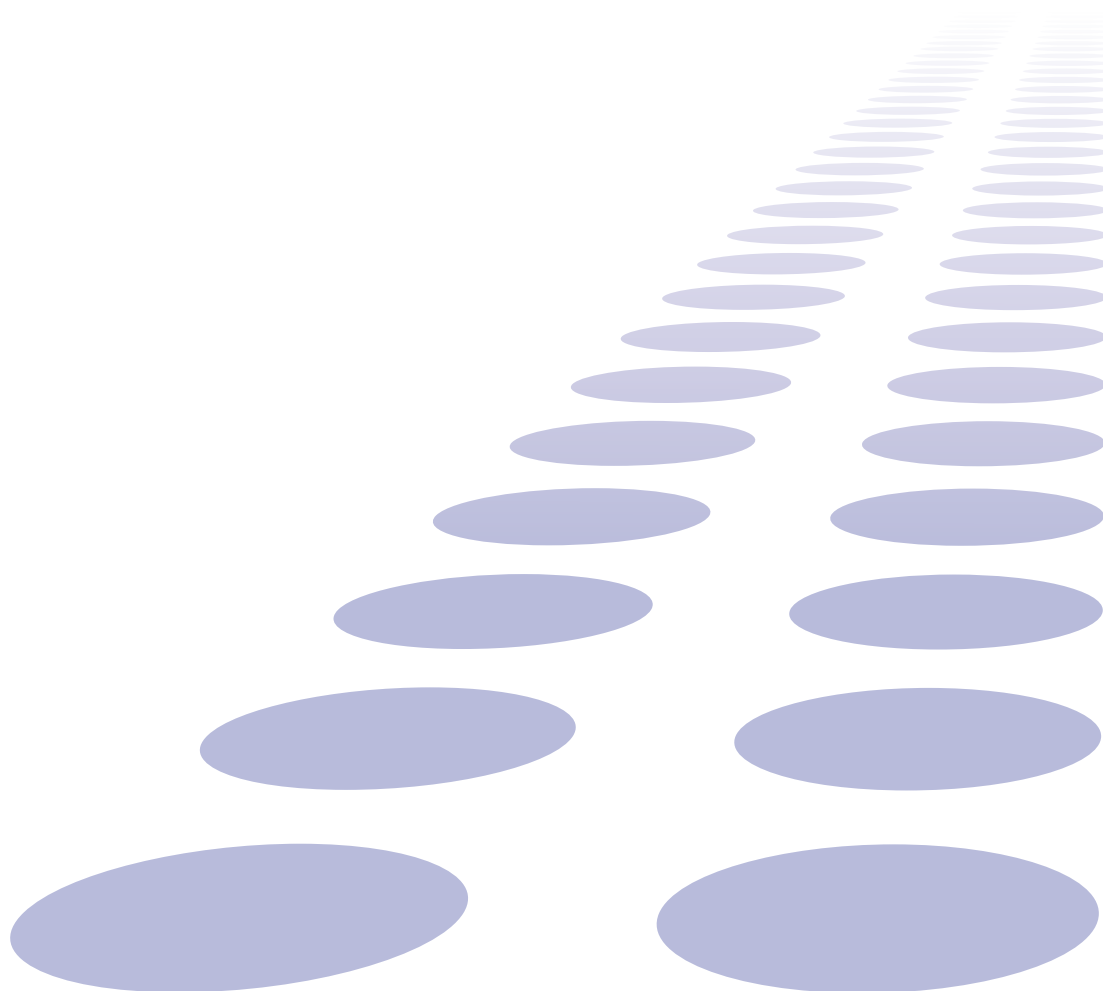


## **Planning for the worst with a comprehensive government resilience solution**



## Introduction

Business continuity and its public sector equivalent, government resilience, is one of the most pressing requirements facing IT managers today. However, how do they achieve the numerous benefits without implementation headaches and a big financial outlay?

Having a government resilience plan makes sound financial sense. It protects against loss of revenue, provides confidence to citizens and protection for staff. In some cases, a government resilience plan will be a statutory requirement. If handled correctly, government resilience will add value to the day-to-day operations of a public sector organisation.

## The business case for government resilience

### Why do I need government resilience?

None of us can foretell the future, but we can prepare for unfortunate eventualities. Disruption to your telecommunications infrastructure can lead to a direct loss of revenue and substantially damage the reputation of a local council or other public sector institutions.

In the banking industry business resilience is considered so important that legal regulations dictate how it is implemented in house. However, for local government the rules and regulations are not so stringent, and yet the implications of a network failure without sufficient backup systems in place does not bear thinking about. A single communications network entails significant and prolonged risk.

High profile terrorist attacks, natural disasters and accidents have placed the spotlight firmly on the security and robustness of government institutions. Citizens need to have a council that is responsive to their needs. The highest goal for government resilience is therefore that citizens never notice a difference in the services they have come to expect no matter what the situation. In this sense “always on” communications and scalability have to be the watchwords for local council IT managers.

### What does government resilience consist of?

Although they are often used in the same context, government resilience and disaster recovery are completely different philosophies. It has often been said that government resilience is like an Anti-lock Braking System (ABS) in a car. It provides features to help you avoid an accident while improving your driving ability.

Disaster recovery, on the other hand, is more akin to an airbag, which may save you from serious injury in a crash. It does not help you avoid an accident and, in normal conditions, it does not provide any added value to your day-to-day driving performance. In an ideal world, everybody would drive a car with ABS and an airbag while wearing a seatbelt. In the public sector, every organisation should have both a government resilience strategy and a disaster recovery plan.

Local councils need to adopt a holistic approach when it comes to total communication protection, using a mixture of resilience, security, availability, recovery and scalability planning which combine to deliver overall government resilience. In terms of IT, a high availability computer system offers resilience to failure by mirroring between two identical servers. A failure of one is automatically detected allowing the other to take over seamlessly, enabling system access to continue uninterrupted.

But in terms of network reliability, backups have to be in place. Government resilience is about anticipating the crises that could affect a public sector institution, and planning for them - whether that be a cut line during road works or natural disaster. Services must continue to function no matter what the circumstance. Government resilience is often considered as a cost centre, increasingly however everyone should consider it as business critical. Forward thinking local councils have realised how accidental and deliberate disasters can expose them not only to risk, but the chance that worried citizens might not be able to get through to emergency numbers.

In light of events such as the Buncefield oil depot fire, many organisations have realised how such a disaster can contribute to reduced productivity and long-term brand damage. Government resilience planning is not simply a cost either. Government resilience experts can identify other benefits in terms of business flexibility and cost savings.

### The technology and its implementation

Public sector decision makers should adopt a holistic management process that identifies potential risks that threaten an organisation. This should provide a framework for building resilience with the capability for an effective response that safeguards the interests of employees and the institution's reputation.

ntl:Telewest Business' networks are built with resilience in mind and many of its council and emergency services customers benefit from multiple connections so that in the unlikely event of one going down, services can seamlessly divert to the backup. The level of resilience can be tailored to meet individual customer needs. It is the stability, scalability and availability of the network that is key to government resilience as it underpins the communication process – facilitating data transfer relating to emergency and enquiry calls. If network connectivity is destroyed, local council and emergency services are likely to be critically hit.

As ntl:Telewest Business has its own, Next Generation Network stretching across the UK it does not need to rely on BT's network. This means it can offer a viable, independent alternative, providing true network backup and strengthening government resilience.

Ethernet networks also address the question of scalability as bandwidth can be increased quickly and painlessly at the request of the customer. West Midlands Police – the UK's second biggest police force – uses ntl:Telewest Business' Evolved Ethernet technology, to provide an advanced network that reaches out to all 120 sites in the region, ensuring scalable and reliable bandwidth to meet its needs now and in the future. Councils and emergency services equipped with Ethernet can drastically ramp up their bandwidth capabilities in case of disaster to meet two distinct needs; they need to be able to respond to peaks in citizen enquiries and cope with increased data traffic diverted from affected sites. And that is the key - government resilience is not just about a backup in the event of a line going down, it is about total support in the event of the unforeseen, including being able to add further equipment or bandwidth quickly and flexibly to meet unexpected traffic peaks or issues.

In the event of a disaster, an Ethernet or IPVPN network enables organisations to centralise their IT and replicate data from whichever of their sites they choose. Citizens' enquiries can be answered without delay. Local council employees should be able to work from home and log onto their VPN, safe in the knowledge that the network is secure and work can continue as usual, albeit off-site. The authorities and the citizens they serve need not be left in the dark in the event of a natural or man-made disaster.

In the event of such an incident occurring IT systems need to keep running, multiple sites must remain connected, employees must be able to communicate effectively and data transfers relating to council tax payments, financial records, payroll and outstanding orders must continue.

ntl:Telewest Business' IP Multimedia service offered over a secure network ensures that employees can work seamlessly and effectively from home. IP Multimedia adds visual options, including video, instant messaging, collaboration and presence indicators to VoIP, bringing them together in an environment of increased usability and manageability.

The mobility of IP networks also enables more flexible and resilient monitoring of camera networks – in the event of a control centre going down, images can be automatically delivered to alternative sites, ensuring security monitoring remains consistently high.

### How do I go about government resilience implementation?

Meeting the challenge of maintaining network connectivity is only possible by working in partnership with a trusted network service provider. To assess the requirements of a communications disaster recovery strategy that suits each organisation, it is necessary to use a range of tools:

- **Risk audit** - review all communications networks and assess potential risks
- **Business impact analysis** - identify mission critical services and prioritise risks
- **Contingency plans** - develop a strategy and outline tactics to manage and respond to a communications failure
- **Resilient network** - invest in technology to protect the mission critical communications capability
- **Government resilience strategy** - develop an approach to deliver a business as usual service to citizens

With the output from these tools, organisations should be able to rank the level of risk from 'critical' to 'high', determining the acceptable period of downtime and subsequent contingency plan.

## Planning for the worst with a comprehensive government resilience solution

In addition there are three key elements to preventing prolonged downtime in the case of a disaster:

- **Resilience** - to prevent the Wide Area Network (WAN) becoming compromised, resilience is required. This means in the first instance that there would be two backup paths to sites holding mission critical data or applications. This would guarantee up time should a JCB in the council car park inadvertently cut through one of the lines. Two separate routers should be on-site to avoid any single points of failure.
- **Security** - privacy is a key element of security, ensuring that outsiders cannot access data. Private lines ensure that there is no opportunity for loss of data in transit. Making sure that data is encrypted adds a further layer of security for traffic on WANs not using private lines, as does the deployment of advanced firewalls. Data storage is also a key factor and company information needs to be backed up on a regular basis and stored off-site so companies can continue business as usual.
- **Intelligence** - companies need management tools that give visibility of network traffic to prevent service drop outs and rebuild damaged data paths quickly in the event of an emergency.

### The practical challenges

Preparation is the key to delivering for a comprehensive resilience solution.

Many organisations underestimate the risk of an event occurring that will disrupt telecommunications. The reliability of modern telephone networks and telephony equipment inevitably lulls many into a false sense of security. An organisation can become aware of just how vulnerable they

may be by conducting a business impact analysis.

This will cover more than telephony; it will help identify critical business functions such as computer, back office operations, data, communications and utilities. Additionally, it will help identify risk implications such as lost sales, potential fines and even lawsuits.

By working together with your service provider to identify any weaknesses you can design network resilience, security, scalability and failover solutions appropriate to your specific needs. This helps with deciding from the start what systems are right for your situation as the practicalities and the financial burden they may incur in the short term are the core challenges facing IT decision makers.

### The public sector needs to take its lead from UK business

The effect of prolonged downtime or loss of private data can be damaging, not just for the council's reputation but also to the citizens it is charged to protect. The moral? Prepare for the worst, even though it may never happen. It is the responsibility of those employed by the public sector to ensure that their systems are robust enough to handle anything that can be thrown at them. True resilience is therefore critical to delivering today's citizen-centric services.

To find out more call **0800 052 0845** or  
visit **[www.ntltelewestbusiness.co.uk](http://www.ntltelewestbusiness.co.uk)**

Part of the Virgin Media Group.  
ntl:Telewest Business endeavours to ensure that the information in this document is correct and fairly stated, but does not accept liability for any error or omission. The development of ntl:Telewest Business' products and services is continuous and published information may not be up to date. It is important to check the current position with your local ntl:Telewest Business office. This document is not part of a contract or licence save insofar as may be expressly agreed in writing. ntl:Telewest Business, Media House, Bartley Wood Business Park, Hook, Hampshire, RG27 9UP. DX4005WP0408

