# Why Business Continuity?

By Steve Yates,
Resilience Director,
Acertia Limited.

Areyoutakingtheissueof BusinessContinuityseriouslyenough?

42% of UK organisations do not have Business Continuity Management in place, according to the Chartered Management Institute.[1] Recent research suggests that cyber security threats are an increasingly serious risk to their business, with nearly a third of UK organisations having been affected by viruses or malicious software during the past 12 months.[2]

According to the London Chamber of Commerce, 90% of businesses that lose data from a disasterareforcedtoshutwithintwo years.[3]

Steve Yates, Resilience Director for Acertia Limited, believes that many British organisations could unwittingly be sitting on a time bomb in the event of an unforeseen catastrophe, be that devastating natural disasters suchas fire, gale, flood, or even man-made.

## Communications and Business Continuity

In a networked world, network communications are the most critical element of your information infrastructure. Communications have become fundamental to commercial operations.
Have you considered how your organisation would manage without telephones or internet access, or how critical email has become? Furthermore, the way we actually use our communication devices has become more complex than ever, in not only our personal, but also most significantly in our professional lives. If disaster should strike, what would be the impact on your day-to-day operations if your communications network ceased to function?

## Imagine there’s no network

There are many feasible scenarios that could lead to a network outage.
For example, a digger could inadvertently cut through your telecommunications cables. Have you ever actually considered the tangible consequences of this, or of any other disaster occurring?

- What if key commercial data was lost or destroyed?
- What if internet access and email were no longer available?
- What if your organisation’s website was down or a virus had infected it?
- What if your call centre was unable to receive inbound or make outbound calls?
- What if your remote offices could no longer be connected?

Serious food for thought, as any one of these could have potentially devastating consequences for your organisation’s viability. Communications networks have today become the backbone of our working lives, so take a moment to consider what would be the real impact on your organisation if yours stopped

*cont’d*

functioning. At the very minimum this would be aninconvenience. More seriously, supply chains would collapse and customer management operations would break down. You would be unable to take orders or even contact your customers – and more importantly, they would not be able to communicate with you. Public sector organisations in particular are charged with being openly accountable and are exposed to frequent media and public interest. Suddenly being unable to communicate or respond would be deemed unacceptable.

The far-reaching consequence of network downtime therefore would be detrimental to the credibility of any organisation,

underlining the importance of Business Continuity.

The chances of a disaster striking your organisation may appear slim but then again, is it really worth the risk of doing nothing to prepare for it? Organisations and individuals take out insurance to cover loss, but that can only provide delayed financial recompense in the event of an incident.

So, what contingency plans can your organisation put in place to ensure Business Continuity? How can you maintain communications with your end users to give the impression of 'business as usual'? Should this plan cover all sites, just your head office, or selected services/products?

*According to the Environment Agency, around 5.2 million properties in England, or one in six properties, are at risk of flooding.[4] The most recent example being the floods in 2014, which affected various parts of the company. According to the Federation of Small Business, small firms lost more than £830 million [5] Local businesses struggled with the cleanup, while 800,000 homes were left without power for up to a week..*

## The communicationschallenge

In order to make informed decisions, it is necessary for your organisation to define its overall service objectives, which will in turn identify key areas of risk with regard to voice, data and internet communications.

When considering Business Continuity, the 80/20 rule is a good way to start. For example, 20% of high risk and mission critical capability requires 80% of the available resources. Organisations must recognise which communications need 100% network availability and those where contingency plans or service level agreements will suffice.

## Identifying areas of risk

To identify operational-critical communications it is necessary to carry out a risk audit. This audit will enable an organisation to define its BusinessContinuity strategy.

The information derived from a risk audit should make it possible to identify communications that are 'critical', through to those which constitute a 'high risk' ifthey are disrupted, and hence must berestored within a 'business acceptable period of time', thereby requiring a 'contingency plan'. These preparations will assist in the development of Business Continuity plans to deliver communications resilience for any service disruption.

*cont'd*

## The meaning of resilience

Unless your organisation is prepared to separate and duplicate all network service and technology elements, both internallyand externally, across multiple sites, then inevitably there will be a service outage at some time. Resilience is required to prevent your voice and data networksfrom becoming compromised.

### Building operational resilience: The seven Rs

One approach for building operational resilience for communications involves following ‘the seven Rs’ methodology:

1. **Responsibility**
   Identify who is responsible for delivering network resilience and establish a Resilience Programme Team that includes internal staff and vendorrepresentatives. Secure agreement onresilience life cycle elements, includingchange management.
2. **Review**
   Identify risks to communication networks. Using the Resilience Programme Team, audit the network by deploying schematics of network routing/cabling and system connectivity.Agree provision, maintenance andservice level agreements. Developchange management, contingency and emergency procedures.
3. **Risk**
   Determine an acceptable level of risk by conducting a risk analysis of physical and logical network components, especially internal and external, high risk and mission critical systems.
4. **Redundancy**
   Highlight which critical communication elements need full redundancy by conducting a business impact (‘what if..?’) analysis, reviewing both internal and external information regarding network design, the network service provider and the network and system-level resources needed for redundancy.
5. **Resiliency**
   Determine what resilient means and its value to the organisation, determine thecost for a truly resilient solution and perform a business case analysis.
6. **Recoverability**
   Identify how quickly mission critical infrastructure elements must be recovered. Do the same for non-critical communications assets and develop contingency plans for those assets whereno resiliency can be provided. Once recovery time frames have been identified, establish service level agreements with equipment andnetwork service providers. Then, establish command and control procedures to manage recovery.
7. **Restoration**
   Establish the amount of time needed to restore full network operations. Activatecontingency plans to restore serviceswithin acceptable time frames asrequired and ensure that management is aware of - and have agreed on - theproposed restoration time frames.

*“Resilience is the ability of a network to withstand internal failures and external events at best without affecting traffic or at worst with a manageable reduction in service level.”*[6]

cont’d

## Not to be ignored – data back-up

Although resilience is widely acknowledged to be the most critical factor in keeping your communications network fully operational, it is also important to bear in mind other areas of your organisation that are at risk, in order to prevent prolonged communications downtime. These include security and data storage, and should also be incorporated into your Business Continuity strategy.

With the former, privacy is a key element - ensuring that outsiders cannot access yourdata. Private lines ensure the clear separacyof data over a dedicated medium withshared mediums, such as Frame Relay providing logical separation of customer data. Ensuring that data is encrypted adds a further layer of security for traffic on WANs (Wide Area Networks), as does the deployment of advanced firewalls. Data storage is also a key factor in Business Continuity - information needs to be backed up on a regular basis and stored off-site so your organisation can continue business as usual.

## Meeting the challenge of Business Continuity

Business Continuity is far too often seen as a cost centre rather than a critical part of modern strategy. The prevalence of this attitude potentially exposes organisations to seriously reduced productivity, or, in the case of the public sector, a failure to meet its service objectives, and in the longer term, potential loss of credibility in the event of a disaster. Any organisation seeking to protect its mission critical communication elements from such events must be prepared to invest time andresource into Business Continuity.

Resiliency is crucial to meeting the challenge of maintaining communications network connectivity in the event of a disaster, and fundamental to this is the establishment of an effective partnership with a trusted network service provider. With the assistance of your telecoms partner, you can conduct careful mission critical analysis of your organisation’s operations to identify key risk areas. From this you can then formulate an effectivecontingency plan which should ensure that you can successfully overcome any eventuality and should guarantee your organisation’s ongoing continuity.

## About the author

Steve Yates is the Resilience Director for Acertia Limited. He is a founding Fellow of the Business Continuity Institute (FBCI) and Fellowof the Institute of Civil Defence &Disaster Studies (FICDDS). Steve is Chair of Business And National Government (BANG) and can be contacted at steve.yates@acertia.co.uk

Sources:

1 https://www.gov.uk/government/publications/the-chartered-management-institute-business-continuity-management-survey – Business Continuity Management Survey 2011

2 *Ibid*

3 Disaster recovery: business tips for survival Information Centre Guide. London Chamber of Commerce and Industry, May 2003

4 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/292928/geho0609bqds-e-e.pdf – Environment Agency’s 2008 National Flood Risk Assessment

5 http://www.theguardian.com/business/2014/mar/05/uk-floods-cost-small-firms-830million-pounds

6 www.odtr.ie – Office of the Director of Telecommunications Regulation – Ireland; 27 September 2001, Document 01/77, Consultation Paper on Network Resilience