



## **The Future of Business Communications**

### **Solutions for Telephony Business Continuity**

#### **Ensuring Business as Usual**

#### **White Paper**

#### **Abstract**

*Disruption to the telecommunications infrastructure can lead to a direct loss of revenue and substantially damage the reputation of a business amongst its customers, suppliers and shareholders. This white paper provides an overview of Contact's technology in respect of telephony business continuity and disaster recovery as well as the issues involved in creating a business continuity plan to protect telephony services within organisations of any size.*

*The solution discussed in this white paper is PBX and telephony device independent and will operate with any existing corporate telecommunications infrastructure.*

Author: Tom Nokes

Marketing Director, Contact Ltd



## Introduction to Business Continuity

Although they are often used in the same context, business continuity and disaster recovery are completely different philosophies. Business continuity is like your Anti-lock Braking System in the 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 the ideal world, everybody would drive a car with ABS and an Airbag while wearing a seatbelt. In the business world, every company should have both a business continuity strategy and a disaster recovery plan.

Having a business continuity plan makes good financial sense. It protects against loss of revenue, provides confidence to share holders and protection to staff. In some cases, a business continuity plan will be a statutory requirement or will be essential requirement for certain forms of insurance cover. If handled correctly, a business continuity plan should add value to the day-to-day operations of your business. IT departments are well versed with the need to have effective disaster recovery plans - to protect mission critical applications and data. They often prioritise budget for tape backup units and fault tolerant servers. Protecting mission critical IT assets is now the 'norm' for every sensible business. But many organisations still overlook the need to plan an effective strategy for loss of telephony services and for the maintenance of Telephony Business Continuity. Yet the costs and consequences of loss of telephony, even for a short period, are high and the likelihood of needing the plan to come into effect are far higher than for a disaster recovery plan.

Loss of contact with customers, suppliers, partners and, even, between co-workers has a detrimental effect on the running of organisations of any size across every business sector. The number one method of conducting business transactions is still the telephone, with some analysts estimating that 80% of all commercial transactions use the telephone.

Although loss of carrier service is uncommon, disruptions can occur that cause normal business processes using a telephone to be disrupted. It's not necessarily dramatic events that can suspend telephony service; a burst water main flooding a building or workmen drilling through a vital utility cable can cut telephony communication and leave a business in a state of confusion. A bad traffic jam due to an accident can isolate your staff from their normal telephony systems. According to the Henley Management Institute, 60% of companies that experienced a loss of normal telecoms for a period of 10 days ceased trading within a year.

This paper will focus on the three essential steps for creating a business continuity strategy and will look at how to construct a disaster recovery plan to protect telecommunications.

## Business Impact Analysis

Many organisations underestimate the risk of an event occurring that will disrupt telecommunications. The reliability of modern telephone networks and telephony equipments 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, lawsuits and lost market share. Business Impact Analyses are often offered for free by some telecommunication service providers and telephony vendors keen to sell additional services or for a nominal fee from independent consultants.



## Contingency Planning

In the telephony area, a good Business Impact Analysis will give an organisation a detailed knowledge of specific requirements for call handling. In the planning phase, documentation of a number of measurements is paramount - including identification of call frequency, volume and type, difficulty and priority in the queue. Furthermore, organisations should be able to determine how calls will be deployed and handled in the event of a loss of telecommunication.

Most companies appoint a recovery team comprised of senior management and team leaders and notify staff of the people on this emergency call list. Another common practice is to create an escalation procedure that activates a set plan, based on severity of an incident, which can be escalated by the recovery team as the situation demands.

Business continuity planning is often part of the normal business model. For example, a call centre operation may have two separate sites. If one site needs to be evacuated due to an emergency, the call load would be routed to the alternate site until the emergency is over. A disaster recovery equivalent could be an empty call centre run at minimal cost that the evacuated staff from the main call centre could relocate to in the event of an emergency. The potential problem here is immediately obvious - as an example, deploying a standby call centre offers no day-to-day advantages to the business since it is in standby and non-operational as long as the business is running normally. If a recovery situation does arise, then staff are immediately functioning, but in an entirely different situation with the likelihood of working with different tools and having to remember different access requirements - all of which does not ensure a seamless continuation of business as usual.

Today, with the growth in mobile telephony, many organisations perceive mobile phones as the potential continuity plan in the event of loss of telephony. However, the mobile phone is often a personal asset of a staff member and continuity planning needs to have a set of procedure for how calls are to be diverted to mobile phones and whether a network operator or company provided voicemail service will be used to catch missed calls. It raises issues of telephony escalation procedures if a call is unanswered and voicemail storage, collection and forwarding since these business telephony features are, typically, not provided in a standard personal mobile solution. It is important to note that, regardless of your recovery plans, both telecommunication service provider and outsourced facilities providers will likely play a role in your planning with various timeframes for activation and costs involved for such services. This dependency on an outside provider in times of disruption is a weak point in the plans and if it can be avoided, by using normal business practices that avoid an outside supplier, it is likely to be easier and more natural for staff to maintain business as usual.

## Testing and Adaptation

For any plan to be viable it must be properly tested and updated based on current business conditions and threats. Testing is often based on a number of different possible scenarios. For example: loss of local telephony, such as a PBX breaking down; loss of a site due to fire or flooding; or loss of the local PTT network. The four broad steps of a business continuity test are: event creation, participant notification, plans enactment and test evaluation. Like a regular fire drill, some companies run these tests at scheduled times or during a live business environment to test both the effectiveness of business continuity infrastructure and recovery team members. By measuring key deliverables, such as switchover time, downtime and missed calls, the recovery team will be able to identify any problems with the plan and incorporate any required improvements.

A far more reliable and less disruptive solution is for business continuity practices to be used as part of the normal business process then testing is made much simpler. For example, if a company uses an intelligent number solution that allows calls to be pulled to another location,



such as a mobile or home phone number, at the request of the users, then testing is done as part of normal working practice.

## Telephony Applications as Part of a Business Continuity Solution

Contact is the leading supplier of intelligent communications solutions. Contact's suite of applications is delivered as On-Premise solutions, Managed or Hosted Services to medium and large Enterprises and Service Providers.

Contact uses packaged applications with both 'standard' and customised solutions, depending on the needs of the client. The majority of Contact customers deploy intelligent numbering as both a business benefit for everyday use and for continuity reasons. Intelligent numbering allows a user to pull calls to a voice-enabled device that can include office, mobile, home, or even satellite phones.

The technology allows missed calls to be captured within a centralised personal mailbox. Voicemails can then be accessed directly - from any telephone, by email as voice attachments, retrieved over the net or even forwarded to another colleague. The adherence to industry standards, plus built-in support for proprietary protocols used by the major vendors, allows PBX's from any vendor to be seamlessly united into a common voice/IVR/messaging interface.

When delivered as a hosted service, the need to maintain customer premise equipment or retain specialist staff is avoided. Hosted services provide a fixed cost for telephony that scales as the business grows. Contact hosted services can also be managed via web-based tools and can be customised to each client needs.

The Contact application suite consists of a range of core products for businesses to improve business communications - a full list is detailed at the end of this white paper.



## Typical Business Continuity Scenarios

Contact technology is entirely software driven and thus provides flexibility in respect of business continuity. The products and services scale from single users at a single site to multinational corporations with international offices. Many Contact customers have built business continuity plans using Contact technology and several examples are provided below to show the scope of these plans.

### *Low Severity Scenario*

A local transport strike has made it difficult for staff to get to work and many are now forced to work from home. Personal Numbering allows these temporary home workers to dial into the system and redirect calls to a home number. In addition, a centralised unified message centre allows home workers to gather missed voicemails and access faxes sent to work via a web browser. This offers a form of business continuity but is deployed as an integral part of the normal operation of the company and has no cost increase for customers already using Contact applications for standard telephony. This functionality can be added into a traditional PBX or IP Telephony system with ease. Intelligent numbering also provides a good continuity solution for other low severity incidents that could include, for example, staff sickness, train station closures or heavy snowfall blocking roads. In all these low severity scenarios, business infrastructure is unaffected but some members of staff are now in another location.

### *Medium Severity Scenario*

A security alert has forced evacuation of the primary business premises. Although business IT systems and infrastructure remain intact, all staff are now outside of the place of business. In this scenario, a first requirement may be to contact all staff to ensure their safety and cascade this information through the company.

Secondly, those staff not already at the disrupted site may need to be contacted and instructed to remain elsewhere and continue to operate business as usual. To handle this during a period of disruption, implementing some form of automation is essential.

The ability to use a personal number to immediately have staff available for calls despite the disruption is the first step. Instant conferencing capabilities at any phone will allow a response team to quickly contact managers and team leaders to deploy a continuity plan. The team may then need to notify all staff of the evacuation and deliver a company-wide SMS to all staff on mobiles. To avoid having to rely on each staff member to logon to an alternative number, the system can be set up to provide an automated alert, instructing staff to initiate the logon to pull all calls that would normally go to their desk phone to their mobile phone instead.

Prior to the security alert situation, a script can be created within the company Interactive Voice response (IVR) system which will, at the press of a button from any phone, invoke pre-planned changes to call scripts to manage appropriately calls normally handled by the main switchboard and redirect calls to mobiles or another office/ branch. This can include the creation of virtual teams of people to ensure critical calls are answered and a team mailbox can be used to ensure calls not answered are kept under the control of the system and passed to the next available team member or a central company team mailbox. In this scenario, all staff are now outside of the normal place of business but, for the customer or supplier, business continues as usual with no changes required from them.

The applications used in this scenario are all applications that are in use during normal business operation and overall costs are a minimal increase based around building the system to cater for increased usage during the period of disruption. There will be an increase in call costs during the duration of the emergency as calls are now taking place across the mobile network rather than



any company lines running at corporate rates, but this cost is not a major expense compared to loss of business revenue due to loss of telephony contact during the period of office closure.

### *High Severity Scenario*

A major fire/flood/gas leak has forced the closure of the primary business premises. All IT infrastructure and telecommunications services are now unavailable. All employees need to be relocated and the time frame till reinstatement of primary premises and critical business infrastructure is unknown. The response team now activates a prepared Contact hosted service at an external hosting centre that takes control of calls to critical business telephone numbers that would normally be assigned to the primary premises. The hosted service has a complete list of intelligent Numbers for each employee and hunt groups for sales, purchasing, human resources, finance and other departments.

Interactive Voice Response handles all calls that would normally be handled by the company's switchboard operator and the service also allows voicemail and faxes to be accessible via web browser. The hosted service maintains core telephony connectivity and can then redirect calls to another fixed location in the event of staff relocation to a temporary business centre or an alternate branch office.

If the Contact hosted service is used by the business as part of its normal working process, this can give a high level of continuity without additional cost. However, this hosted service can also lay dormant until it is needed with an only a small monthly retainer fee to maintain the service in this 'standby' mode. The Contact hosted service uses a number of communication carriers to ensure that the Contact service remains available and supported, even if a fault occurs within a particular carrier network, on a 24/7 basis. If this scheme is used as a disaster recovery scenario, then the customer needs to maintain accurate records with the hosted service of staff intelligent numbers and caller groups to ensure that switchover can occur smoothly.

## **Using Hosted Services as a Business Continuity Tool**

All of the telephony applications discussed in the scenarios above are deliverable either as Customer Premise based solutions or through Contact Hosted Services. If a company location is in an area considered at high risk of a major severity disruption, a cost effective solution to ensure business continuity is to deploy a hosted service based solution.

This solution could provide business continuity as a hot standby hosted service that could automatically be switched over to cover key incoming calls to the central business number on demand. Alternatively, it could be provided as an ongoing service used for more critical resources to ensure disruption to the main premises did not disrupt communications for key personnel or key business lines.

## **Conclusion**

Recent events have brought the issue of business continuity to the forefront for business managers across a wide range of organisations. There are no good arguments for NOT conducting a Business Impact Analysis - even an internally run, low cost study using rough numbers will easily provide a compelling argument for creating a business continuity plan. For savvy organisations aware of the issues, business continuity is often just part of the everyday working practice. Features like intelligent numbers provide both continuity and added business benefit for a whole segment of the business community.

At the present, a business continuity plan may be an optional process but, as a leader in corporate governance, the law is increasingly making it mandatory for organisations with certain market sectors to have a clearly defined continuity plan - especially within the financial sector. New technology and deployment methods such as hosting means that building a business continuity plan to protect telephony is less complex and less costly than at anytime in the past and

## White Paper



Contact has the experience, applications and services to help meet the needs of organisations of all shapes and sizes.