

## LEARNING THE LESSONS FROM MANCHESTER...

### Case study

*The recent widespread loss of telecommunications services experienced by organisations in North West England has demonstrated how important it is for businesses to ensure that their business continuity and disaster recovery plans include effective measures to protect against telecoms failures.*

### Monday March 29<sup>th</sup> 2004

Business managers in Manchester wake up to the news that there has been a fire in a tunnel underneath the junction of George Street and Princess Street in Manchester city centre. It soon becomes clear that, what had at first appeared to be a limited local issue was in fact having knock-on effects on the whole of British Telecom's network across North West England as well as impacting upon the services of other telecoms providers. In total, 130,000 landlines across the region were put out of action for the whole day and communications problems continued throughout the week.

The incident came just a month after the Business Continuity Institute published the results of its annual joint survey with the Chartered Management Institute. This found that telecoms continuity is now the highest business continuity concern for businesses. 62 percent of respondents stated that they were concerned about the threat of disruption to telecoms and 23 percent of respondents had experienced loss of telecoms service over the previous year.

### MANCHESTER: RESPONSE AND RECOVERY

Various business recovery centres around the North West region were in action as a result of the Manchester outage. For SunGard Availability Services the incident generated a number of customer invocations and also impacted the company's own Stockport facility, resulting in the need to rollback from Stockport to other SunGard recovery facilities in the vicinity. Warrington was the main alternative centre but Normanton and Coventry were also utilised.

SunGard has made a multi-million pound investment in its Workplace facilities nationwide to enable seamless rollback and client transition between facilities. This is underpinned by an ATM network, which connects all 20 of SunGard's UK facilities and which also links to the London high-bandwidth ScaleNet optical network. To significantly reduce local area network restore times, SunGard has installed 5,500 Dell PCs nationwide in a desktop technology standardisation exercise to ensure that customers have access to machines with an identical high specification, regardless of which recovery centre they are relocated to. Desktop conformity and the adoption of sophisticated imaging methodologies enables rapid deployment of desktop environments in a disaster which, as well as reducing restore times, also enables customer images to be operable in any suite or location for enhanced service flexibility and efficiency.



SunGard has also implemented an advanced telephony system which has been rolled out to all of its UK Workplace Recovery locations. SunGard customers are able to access the improved service with no change to their current fee.

The delivery of incoming calls to the right person has long been a problem in business continuity terms, due to the technological complexity and sheer increase in the number of calls received following an incident. However, SunGard's recent investment in new telecommunications technologies ensures that customers' entire telephony environments – including Direct Dial Inbound (DDI) – can be remotely restored to any recovery facility.

In addition, SunGard has developed its own software-based methodology that overcomes the issues of supporting multiple customers simultaneously, without impacting the recovery of those customers.

The Manchester incident was the first large-scale invocation of the upgraded Workplace services and provided an opportunity for the company to 'put its money where its mouth is'.

Royal & SunAlliance was one SunGard client that invoked its business recovery services during the incident and Ian Houghton, the company's UK Continuity Manager, agreed to provide a run-down of the company's experiences during the incident.

Royal & SunAlliance is a leading international insurance company headquartered in London, but with regional offices close to Manchester city centre. It is one of the world's oldest and most well-established insurance groups and writes all major classes of property/casualty and life insurance. The Group was established 300 years ago, has operations in over 50 countries, covers risks in over 130 countries and has more than 20 million customers. The company has had a long history of successful business continuity planning, and gained valuable real-world experiences when it was at the epicentre of an IRA bomb attack on Manchester city centre during the 1990s.

The benefits of post-incident debriefing are well understood by Royal & SunAlliance, with all key players in any invocation gathering after the event to discuss what happened, to discover what aspects of the business continuity plan worked and which failed and to brainstorm and document the changes that need to be made. The following is the result of the Manchester debrief and highlights some valuable lessons learned:

## TIMELINE

### DAY ONE: Monday March 29th

- **3.20am:** Incident commences.
- **8.00am:** Royal & SunAlliance security staff discover that there is a problem. They then pass this information on to the IBM Facilities Management team, who are responsible for the outsourced Royal & SunAlliance telecoms infrastructure, and to Royal & SunAlliance's own business continuity team.
- **9.30am:** The Royal & SunAlliance control management team has its first tele-conference meeting. (The term control management rather than crisis management is preferred by the company, since it has more positive connotations.)
- **9.40am:** The control management team makes contact with SunGard and immediately invokes its business continuity arrangements. A decision is made to use SunGard's Warrington facility as the main recovery centre, since the nearest centre at Stockport has been impacted by the telecoms outage. The Normanton and Coventry facilities are placed on standby. Places for 800 staff from central Manchester and 40 from Cheadle will be required.
- **9.53am:** SunGard confirms that everything is in place and the recovery swings into action.
- **10.07am:** The Royal & SunAlliance control management team receives a call from the SunGard communications team to determine what bandwidth will be required.
- **10.15am:** Bandwidth established.
- **10.30am:** Energis, Royal & SunAlliance's main telecoms provider, has now diverted all lines to Warrington, including fax DDIs, something which many perceive as an 'impossible' technical task due to the difficulty of clearly determining what is a voice and what is a fax call.
- **10.30am:** The Royal & SunAlliance control management team initiates a search for further accommodation in the area, should it prove to be necessary.
- **11.30am:** The first Royal & SunAlliance employees arrive at Warrington. Only a few technical staff have been deployed, with the aim of getting live systems installed, established and tested. One of the lessons the organisation learned from its Manchester bombing experiences was that it is a mistake to try and get frontline staff over to recovery facilities too quickly, since this can result in frustration and confusion.

- **12.00am:** All telecoms services are fully operational and servers and desktop PCs are in place. All desktop PCs had a previously created 'ghost' image prepared. This made initiation and preparation of recovery systems much quicker.
- **1.00pm onwards:** Crisis communications methods are initiated to ensure that all staff, clients and brokers are aware of the situation and to assure them that it is under control. A press script is prepared in case of enquiries by the media and an incident hotline established for employees to use.

At the end of the day, Royal & SunAlliance had configured routers from scratch, moving communication traffic from Manchester to Warrington – providing WAN connectivity. This led to 80% of the servers being moved to Warrington and more importantly, 100% of desktops were operational. As telephony was being swung over to Warrington, this meant Royal & SunAlliance was ready for 9:00am the next day.

Drawing to a close and Cheadle was operating at 30% systems efficiency, including five telephone lines. In Oldham, 'phase one' was underway, trying to establish 50 desks and chairs. Also, Regular conference calls are held throughout the day to assess the situation and to coordinate response.

### **DAY TWO: Tuesday March 30th**

At the beginning of the day, telephones had been transferred over to Warrington and were fully operational for 0900 start, with all servers on site and fully operational. 76 frontline staff are deployed at the Warrington facility to make and receive emergency calls and to help prove that the system is working correctly.

In Warrington 220 staff were expected to arrive on Wednesday – full occupation was anticipated by Thursday/Friday. To coincide with this, 50 workstations were placed in Mercury Court in case of Manchester overflow.

Meanwhile, Cheadle was operational and stable. SunGard Normanton now escalated to full standby (350 seats) in case of a Liverpool and Manchester overspill. The Liverpool Campus SCM/UK Continuity teleconference identified potential WAR solutions due to unavailability of SunGard Warrington and Stockport. Also, the Belfast WAR test was scheduled for w/c 5 April, however it was postponed to avoid potential resource and technology conflicts.

Staff incident hotlines were updated and crisis communications continues – every three hours staff and brokers are updated with information on the current situation.

### **DAY THREE: Wednesday March 31st**

**Full occupancy** – all employees that are available have now been relocated at the various recovery facilities. BT has reinstated 65 percent of normal bandwidth with an estimated



completion by Sunday, almost one week after the incident occurred. However, no guarantees can be made about this so Royal & SunAlliance decide to keep staff operating out of the recovery facilities for a further week.

270 staff fully operational in Warrington. This included both Claims and Underwriting Teams who are now up to strength for their immediate needs.

The UK Continuity Team met with local SCMT and on site team members this morning and carried out site visit. Even more rewarding was that Brokers and Willis Network have heard of excellent recovery and wished to visit the site next week. This provided an excellent business opportunity.

Nearing the end of the day and a Health & safety and security review was undertaken. A local team was to undertake H&S briefing for staff. The hotline was once again updated. Unfortunately, the network (IPX) problem that is preventing surveyors from downloading their reports is still unresolved. Energis, SunGard, BT and IBM are all still on the case and have developed a fall back plan if this is not resolved by the evening.

#### **DAY FOUR & FIVE: Thursday & Friday April 1st & 2nd**

Over these two days there were 360 to 400 staff in Warrington and all was stable. However, there was still an issue with the surveyor's dial-in system, but this was resolved late Friday morning. IBM had been told to stand down over the weekend to rest and reduce any fatigue, while BT was still hoping to have full service restored by Sunday. Royal and SunAlliance took the decision to move back to Manchester on the Bank Holiday Thursday in order to stabilise, recuperate and plan in detail.

#### **LESSONS LEARNED**

During the Manchester telecoms failure post-incident debriefing Ian Houghton identified crisis communications as an area for improvement. "Obviously, the loss of telecoms services over such a wide area had a knock-on impact on our crisis communications capabilities," he states. "It made contacting the whole database much harder and a longer process than anticipated. We also learned that 'less is sometimes more' – perhaps we tried to get too much information across in our messages. Sometimes a short clear message giving just one or two key facts is better than a longer more detailed message."

Rather than the expected prime recovery site being Stockport, less than ten miles from Manchester, all staff were relocated to SunGard's Warrington Recovery Centre.

"SunGard's recovery centre rollback system worked well," says Ian. "However, we did learn some lessons, one of the main ones being the importance of assisting in the logistics of getting our staff to recovery centres. We found that it is probably more effective to allocate staff to a recovery facility based on proximity, rather than job function. Keeping work teams

together may be less important than getting people quickly behind desks. It also helps staff with their own domestic arrangements if we can minimise their travelling times.”

**Other issues identified were:**

- The importance of maintaining compliance with health and safety and other business regulations at recovery facility sites. For example it is important to ensure that there are enough first-aiders on site and that staff have been briefed on fire safety and evacuation procedures at the recovery site.
- The importance of testing - Royal & SunAlliance test business continuity plans at least twice per year and as well as the problems that the tests can identify they also ensure that staff are familiar with the process, know where they are going and can quickly and calmly get down to work in the recovery facilities.
- The importance of flexibility - Royal & SunAlliance give their business continuity management team the authority to make spending decisions during crisis situations. This means that rapid response can be made to unforeseen scenarios.
- The importance of a friendly face. During a crisis the more that familiarity can be injected into what is by nature an abnormal situation, the better. This helps to reassure and calm staff. Royal & SunAlliance ensured that one of their regular security guards was dispatched to each recovery facility, to welcome staff and to provide a ‘friendly face’ upon arrival.
- Royal & SunAlliance made an immediate decision to invoke their business continuity measures. This was endorsed by SunGard as the right thing to do. It meant that business as usual was achieved more quickly than if just a ‘standby’ had been declared. “Equivocation may seem a safer first step giving time to assess the situation, but it can also slow down the whole process quite dramatically,” explained Ian Houghton. “When downtime costs such a large amount per hour you can’t afford to take too long in making the invocation decision.”
- People are vital. “Good plans are important, but teamwork, good communication and flexibility are vital,” says Ian. “The best plans in the world will fail without the right people, without the right training and without the right attitude.”
- The importance of prioritisation. Royal & SunAlliance was able to make good decisions about the recovery priorities during the Manchester incident. This was due to its previous testing experience and its effective business impact analysis work.

The Manchester incident shows just how vital telecommunications is to the modern company. Telecoms resilience is an issue that no company, whatever its size, can afford to ignore. Convergence of telecoms and IT systems means that many mission critical processes are dependent upon the telecoms infrastructure and loss of telecoms no longer just means that customers hear the engaged tone or a pre-recorded message, it means that data

processing no longer takes place; that replication and failover systems are compromised; and that home workers and divisional offices can no longer access data and applications. It means that the whole business is brought to its knees. So, how do businesses go about protecting their telecoms infrastructures?

### TELECOMS CONTINUITY PLANNING

A recent UK government publication provides an excellent resource for this area of business continuity planning. Entitled the 'Good Practice Guide to Telecommunications Resilience' and published by the National Infrastructure Security Coordination Centre (NISCC) the document makes four key recommendations:

#### Organisations should:

- Identify those communications systems that are deemed mission critical and which carry a high risk to the business if they are disrupted.
- Wherever possible separate out the high risk services from those that only carry a medium or low risk to the business if disrupted.
- Understand the architectural options for separacy and diversity based services e.g. what does 'end-to-end separacy' actually mean.
- Recognise that high availability and high resilience services will cost more than standard services, and do not use cost as the main criterion when procuring these services.

The NISCC report highlights the issue of the 'local loop' as being one of the main areas of concern, and this was well-illustrated by the Manchester incident:

“One of the principal areas of concern is the route congestion between customer premises and local exchange or Point of Presence (POP),” the report states. “This is of particular concern in built up or high-density areas and is often a classic example of a single point of failure. Due to the historical position of BT as the incumbent telecommunications provider before privatisation, the 'local loop' or last mile in the majority of cases is a BT asset. Local Loop Unbundling (LLU) obliges BT to allow other provider's use of these assets, resulting in third party providers selling circuits over the same cable routes as BT. As there is no requirement for either provider to discuss the use of these circuits with the other, they may be unaware that the customer possibly intended the circuits to be separated. In this way the customer may be lulled into a false sense of security. True separation, or separacy as it is known, in this example would have been possible by asking one provider for two separate circuits. It is worth noting here that buying two similar circuits from the same provider may actually be more economical than buying one circuit each from two providers. This in turn, however, raises concern over the dependency on a single provider.”



NISCC highlights two further key factors in telecoms resilience:

**Carrier redundancy**

Companies sometimes sign-up with more than one telecommunications company in the belief that this will provide continued service should one of the provider's services fail. However, this may not provide the expected redundancy since many providers simply resell services and have no physical network of their own. If background checks are not made, it could easily be the case that both providers are using the same infrastructure.

**The last mile**

"The 'last mile' (between local exchange and customer premises) is the key to the resilience of a business telecommunications network" states NISCC. The provider's telecoms network has a high level of built in resilience, normally resulting in few failures. However, the last mile connection to the customer is usually a single point of failure, often because there is simply no alternative route. It is often the part of the network which is most exposed to external interference or physical damage.

It is clear from the above that business continuity managers need to either gain an in-depth knowledge of their company's telecoms infrastructure and also of the intricacies of their telecom provider's network, or he/she needs to employ the services of an experienced business continuity consultant.

**REFERENCES**

<http://www.niscc.gov.uk/Guide%20to%20Telecommunications%20Resilience.pdf>