Cloud Direct

Case study

Chaos averted as fire wipes out UK head office - communications recovered in minutes

Our client

For the past three years, Cloud Direct's business continuity (BC) plan has protected the critical IT systems of our eCommerce client.

Operating worldwide, our client had more than 400 staff in their UK head office.

The disaster recovery solution

As part of their BC plan, our client is also protected by our Disaster Recovery (DR) platform. It protects their core communications and business information systems, including: email, core file servers, CRM, customer help desk, ticketing information, HR and finance.

Separately, their internal software development systems are protected by backups which, if necessary, could be used to rebuild them.

The disaster

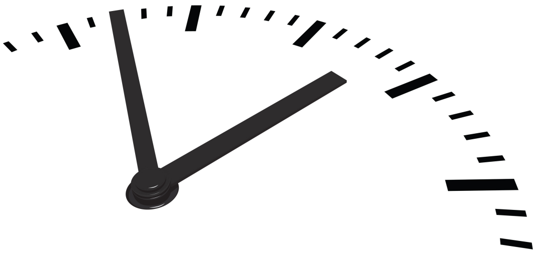
Sometime around 19:30 on Monday 15th April 2013, a spark ignited in the electrical riser of the company's UK head office. Fire quickly swept through the building and soon took hold.

It took the fire brigade 12 hours to get the blaze under control.

When the fire brigade was finally able to assess the damage, they reported that the fire had destroyed all electrical infrastructure, caused fire and smoke damage to four floors and destroyed part of the building's roof.

From the time of the initial fire alert, it was evident to our client that the building would not be usable for business purposes – at least not any time soon.

Critically, from an IT point of view, the state of their servers was a big unknown, and staff weren't allowed access to the building for another 24 hours.



For a global eCommerce company this could quickly have spelt disaster. However, because they had our DR solution in place, the business could pick itself up immediately.

Their initial challenges were to:

1) Get IT services working again
2) Organise alternative offices for their 400 staff
3) Move staff over to the new systems and facilities.

The recovery

Our client phoned our emergency contact line at 21:45 that evening; he passed the security checks, explained the situation and requested a full invocation of their IT services.
Within ten minutes of this first call, Cloud Direct's DR engineers had triggered the automatic, full service invocation process.

Once started, the standby systems booted up one of the remote rescue platforms, and systems

Within 45 minutes of our client invoking the DR service, they were logging back in to their recovered IT systems. They had instant access to core company information - for staff and customers - and the communications systems to contact both. Outbound emails worked immediately, and inbound emails started arriving within the hour.

were up and running within 35 minutes. Rescue servers were automatically brought up in a correctly configured network, with secure user access set up and ready to go. Configuration automatically repointed our client's Internet 'DNS' addresses so web systems and email addresses quickly switched to the recovered servers.

This automated process worked exactly as expected. Our client just had to make one phone call to get the system recovery going and wait 35 minutes before staff could log in remotely.

The simplicity of this approach brought clarity and order to what might otherwise have been the start of chaos. It gave staff the information and tools they needed to start handling the business recovery.

Because the fire happened in the evening, our client's IT staff were able to use the night to organise themselves and warn colleagues that they would need to implement their elements of the business continuity plan. Staff contact details were all available on the recovered systems so phone calls could be made to brief staff for the morning.

The business emailed an initial communication to their customers, alerting them of the fire and reassuring them that they were in control.
By 10am on Tuesday 16th April, around 12 hours after first calling Cloud Direct, the client had 120 of their core staff logged into the recovery systems from home. This meant they could communicate with customers and carry on all non-software development activities. To their customers, it looked like the business was operating pretty much as usual.

Alternative offices

Having got their core IT systems working again, our client's next challenge was finding suitable alternative office space. As part of a larger group, their BC plan dictated looking for space within group offices or via local serviced office providers.

By the end of Tuesday, they had found space for about half their teams in other regional offices and got agreement from DR partner, Regus, for a short term office rental for the remaining 200 staff.

Our DR platform provided secure network connectivity to the Regus and the regional offices. Local access was working again.

Resumption of remaining software development systems

The fire brigade was finally able to allow our client access to their original office on the evening of Tuesday 16th April. They discovered their IT servers to be contaminated with smoke, but otherwise they worked OK and did not appear to be damaged.

As our DR service had solved the immediate IT problem by replacing core systems, our client was then able to calmly and strategically evaluate how best to get their other systems working and return to their local live service.

Connectivity and security company, Level 3, had already provided the client with their core networking, so the obvious location for the servers was in a Level3 facility. That was arranged by Thursday 18th and the DR team provided a software copy of an enabling server to make the service work in the new location.

For speed, this was done by hand and the images exchanged on a USB hard drive at a junction on the M4. As the core systems were securely functioning on our rescue platform, the client was able to now prioritise their software development servers. They started lifting and shifting them to Level3 in Slough, with a plan to then run a rolling programme of professional batch cleansing.

The last key challenge was to securely network the recovery systems into the new servers in Level3 and to provide onward links to our client's new Regus serviced office, the regional offices and their international offices. This was a reasonably tricky piece of networking but because the DR system had created the core connection immediately on invocation, our client and our DR team were able to take time to think through the requirements and implement the correct solution.

By Friday 19th the software development servers were back in action. By Monday 22nd April, absolutely everything – including 85 servers – was back up and running.

Longer term support

After the initial recovery, our client gave us a longer term support role. We then implemented a data backup service so our client had access to both an on- and off-site copy.

Next, we re-implemented the DR service to another Cloud Direct recovery platform. This effectively gave back DR protection to the client for the live systems.

Within a week, our client had all services working fully and all protection back in place.

Client reaction

The recovery of the client's systems and business, went so well they were able to get their staff working again within a few hours. They had full recovery within seven days of a total facilities and systems loss.

According to their chief operating officer, the reaction from their eCommerce customers was amazingly positive – despite the disruption they experienced. Many congratulated them on their professionalism.

Extended migration of the recovery platform

One of the great advantages of the Cloud Direct solution in a disaster, is that it solves the initial IT problem immediately. So business staff can get back to work, and IT staff are free to think strategically about rebuilding their services for the long term. Our client avoided time-based, knee-jerk decision-making. Instead, they decided to turn the disaster into an opportunity to upgrade and rebuild some of their systems, as part of the planned migration of services back from the Cloud Direct recovery platform.

As a result, migration took around nine months, and they were back in their completely refurbished offices two months before the last email servers were moved back to their own systems.

How well did the recovery go?

The recovery of our client’s core servers went exactly as we would have hoped.

They were able to get back to business quickly, make better decisions and take faster actions to guard the long term interests of the business.

However, the real test was how their business fared through the incident.

A key decision-maker during the process said:

“… It simply saved the business”.

He also informed us that, despite the fire and all the ramifications that followed, the business hit all their financial targets for 2013.

From a commercial point of view, the fire had no effect on their long term performance.