DISASTER. WHAT DISASTER?

Good planning means you won't get caught short

By Nigel Wright, Managing Director of Converge Technology Specialists

When fires raged underground in Holborn in London in April this year, few businesses were prepared for the impact this would have. The London Chambers of Commerce estimated the cost to have been in the region of £40m.

None of the buildings caught fire and, thankfully, no one was hurt, but electricity and gas services were cut as the underground fires took 36 hours to control; 5,000 people were evacuated for safety reasons; shops, courts, offices, theatres, hotels and restaurants stayed shut until power was restored; and the main Holborn road reopened some weeks later, allowing businesses to eventually begin to return to normal. An underground electricity fault turned out to be the cause of the London fires. But businesses needed cutting-edge technology to respond to and deal with the challenge of such widespread business interruption.

Preparation is everything

Companies operating on the Cloud would have come through with a distinct and competitive advantage. They were able to pick up where competitors left off as staff were able to work remotely and on systems that were fully updated and worked in real time. All that staff required was a PC or laptop – and they could work from anywhere. In those crucial 36 hours, business continuity plans were well and truly tested. The virtual office and business as usual became a reality for the organised and prepared, despite the very challenging circumstances.

> **"Business as usual became a reality"**

Putting this into perspective, a law firm with 50 fee earners, charging £150 per hour on a 5-hour fee charging day would have lost £187,500 based on a 5-day downtime.

We have worked with clients in situations that would make the blood of most managing partners run cold: a junior member of a client's IT team deleted their virtual server; and another suffered potential business outage due to an air conditioning unit leaking into their office. Perhaps the most likely threat to firms is a computer virus wiping out records or rendering their IT useless. This was the case for one firm affected by the Cryptolocker virus. Luckily for them, a disaster recovery plan was in place (via continuous backup) and the firm was able to return to a point an hour before the virus hit, and get fully up and running within a matter of hours, thus ensuring business continuity.

How would your business have coped in the same conditions? Would you have been able to pick up, dust off and crack on, or would you have had to shut down, put in a claim for loss of earnings and work out how you were going to get back to business as usual?

A duty of care

Of course, law firms are required to provide a duty of care to clients, with a proven business continuity plan in place that outlines how they will continue to trade should the worst happen. It's a requirement in the Solicitors Regulatory Authority's code of conduct.

The SRA stipulates that all law firms must:

- Provide a proper standard of service to clients;
- Behave in a way that maintains the trust the public places in firms and in the provision of legal services;
- Comply with legal and regulatory obligations and dealing with regulators and ombudsmen in an open, timely and co-operative manner;
- Run a business or carry out roles in the business effectively and in accordance with proper governance and sound financial and risk management principles; and
- Protect client money and assets.

Data security and protection is the top priority for UK law firms and a solid, proven and tested disaster recovery service forms part of the process of securing data. Data security breaches can warrant hefty fines, create distrust and taint reputations. It isn't unknown for corporate clients to ask law firms to demonstrate the effectiveness of their data security and disaster recovery plan as failure results in reputational issues in the 24/7 culture we're all now part of.

Indeed, with the SRA code adhered to, firms must also ensure they comply with data protection rules set out by the Information Commissioner's Office, which has taken to making examples of firms that fail to protect their business with appropriate safeguards. Increasingly, Financial Conduct Authority regulations are being forced onto law firms and conveyancing firms, which are stricter than SRA rules.

Have you done enough?

But many firms erroneously believe that simply backing up documents, emails and case files is a job well done, a disaster averted, the compliance box ticked.

The process of business continuity management involves an evaluation of the potential risks that could lead to business interruption. Disaster recovery is your response to an event and also includes how you handle your clients, the media and the public at large. How you deal with disaster recovery – your ability to detect a problem, assess its impact, readiness and speed of response – will determine the overall reputational damage to your business. You may as well close down if you lose the confidence and trust of your market.

Disaster Recovery as a Service (DRaaS) is an essential component for all busy law firms focused on client needs. It replicates and hosts your physical servers through a third-party to provide immediate back-up availability in the event of a man-made or natural catastrophe. This is very useful for small to mid-size businesses that lack the necessary expertise to provision, configure and test an effective disaster recovery plan. You won't need to invest in, or maintain, your own off-site IT disaster recovery solution as it is 'built-in' to your Cloud. All that you and your firm needs is an internet connection to access all your data and applications, removing the risk of downtime through local disruption and disaster, and guaranteeing a continuous level of service to clients.

Of course, outsourcing and handing over data to others introduces other very important risk assessment requirements. It is a distinct advantage to use a UK-based DRaaS provider because they will have access to UK-based data centres. These are

compliant with much better internationally recognised security standards and power back-up systems than a physical server. Many firms moving to the Cloud find that, far from adversely affecting their obligation to clients, it can underpin and guarantee delivery of that obligation, as well as providing the DRaaS that they require.

Today, more than ever, as data volumes massively increase and networks become more complicated and testing more onerous, a well thought through disaster recovery plan that considers every possible scenario is essential. Firms need to be able to robustly answer:

- How frequently do we test our disaster recovery plan?
- Is our test to destruction thorough enough?
- How well does our system stand up to threats?
- Do our people know who to reach, what to do, and when they should invoke the business continuity plan?
- Do our people know how to reach the right decision maker and raise the alarm to ensure business as usual or, at the very least, as close to business as usual?
- What do we regard as the right and affordable recovery time objective (RTO)?

But where do you start when it comes to testing systems to destruction? Law firms need to think about and plan for the following:

Test for 'worst case scenario'

An annual, all server shut down, should be the minimum test you undertake, and there is no time like the present. Your clients, panel referrers, quality standards, or management team may require it to be more often. A half-hearted test will not satisfy the above and it should not satisfy the business – always test for the worst case scenario. Consider a fire, a terrorist event, the sudden incapacity of the IT leader or key decision maker and look around you for threats to your business. It could be cybercrime and business sabotage, it could be a natural disaster such as the flooding of a river into your premises, or it could be man-made and as simple as someone spilling water onto your server or a major power cable cut during roadworks.

Include a representative test group

Junior and senior staff should be included in testing the firm's resilience to disruption, and how quickly they can return to fee earning work. Run the test during a time when it is least disruptive, such as an evening or at the weekend, but ensure the test is realistic to build confidence in your business and in your staff. Obtain feedback from staff about any lessons learned from the experience. What were the gaps in your defence? Where were the weak spots? Did everyone know what to do and how to react or respond?

Measure how quickly your firm returns to 'business as usual' – and adapt if necessary

Test how well you meet your RTO – the amount of time lost that your business can potentially sustain. If you fail to meet your RTO, look at ways to reduce it and test and test again. When disaster strikes, being able to easily open and find crucial documents can make the difference between a few hours and a few days in lost fees, as well as keeping reputations intact.

Lexcel as a Practice Management Standard and the Law Society have reacted to the growing threats to business continuity by including a useful business continuity management toolkit. The kit includes signposting to information on the Governments Cyber Essentials Scheme launched in June 2014, the ISO27000 series of International Standards on Information Security Management, and useful Law Society Practice Notes and on-line webinars.

With the right approach, a business disaster can be minimised if not diverted, reducing the impact on down time, costs and reputational damages to your business. The time to act is now.

About the author

Nigel Wright is MD and founder of Converge Technology Specialists – a provider of managed and hosted IT services and the only cloud provider dedicated to UK law firms. He's spent 18 years delivering technology services to professional firms of all sizes.

www.convergets.co.uk