DEALING WITH DISASTER

IT failure may not just be inconvenient – it could damage your reputation. But get your disaster recovery plan right, says **Ian Cockburn**, and you could enhance business in the process

CORBIS

As IT plays an ever more critical and pervasive role in all aspects of business, it also presents significant risks that need to be managed. Imagine your firm or one of your clients loses the use of their systems for a week or more – due to a virus, or a storage area network (SAN) or server failure. Now imagine that happens in January, as you approach the tax filing deadline, or just as your client enters its peak sales season. Unless there are robust arrangements in place to recover full IT functionality within a short, pre-defined timescale, the damage could be severe, even fatal.

A disaster can be anything from hardware failure and loss of connectivity to flooding or fire. The IT failures at Natwest and RBS this year serve as a timely reminder of how wrong things can go. Any extended period of downtime can have dire consequences for small businesses. Yet, research from last year found that 10% of respondents had no disaster recovery plan in place.

The survey of IT managers, carried out by *Computing* last year, shows that most SMEs are not wholly embracing suitable disaster recovery plans. Many are reliant on inadequate tape back-ups, rather than protecting their businesses with automated off-site back-ups of systems and data, and comprehensive and regularly-tested disaster recovery arrangements. While the majority of those surveyed said they did have a plan in place, 53% only review the plan annually or less frequently. External accountants are exceptionally well-placed to provide independent, professional advice on this issue, but unfortunately many professional firms may be equally inadequately protected themselves.

At the very least, the absence of adequate back-up and disaster recovery arrangements will mean the firm is non-compliant with specific requirements of the ICAEW's Quality Assurance Department and of the Data Protection Act regarding its own IT systems. In addition, firms could be exposed to unnecessary risk should one of their clients go into liquidation following a computer disaster. Just as continued access to necessary finance is vital to the concept of 'going concern', continued access to systems and data is also essential to survival. As IT dependency increases, so does this risk.

Firms may have a partner designated as responsible for IT within the practice, but that partner may not have any specialist knowledge in IT. It may be advisable in such circumstances to use external expertise to ensure that the firm is adequately provided for. The knowledge thus gained can also be used to provide advice to clients, while protecting or enhancing fee income and client retention.

CLOUD-BASED SOLUTIONS

Cloud-based solutions are now well-established and, if carefully selected, can provide fully-automated protection at a very reasonable cost. However, good systems are complex and need to be very robust and well-supported. Half of the respondents in the *Computing* survey said they'd consider the cloud for disaster recovery but a considerable 29% said they wouldn't, the main objection being security fears. Concerns about the security and reliability of cloud-based solutions can be satisfied by applying the following selection criteria:

- Choose a solution based on proven and widely-used back-up and restore software, with the necessary high level of encryption and security and the necessary level of support from both the service provider and the software developers.
- Know exactly where the off-site back-ups will be stored. This inevitably means 'private' rather than 'public' cloud. Inspect the location to ensure it is a high-security Tier 3 (or in certain cases, Tier 4) data centre with a suitably high-capacity bandwidth availability.
- Ensure the contract includes regular testing of the full server restore process so that reliability and timescales are fully understood. Ensure the restore service is backed by high-quality, in-depth engineering support.
- Ensure the back-up maintains multiple data revisions, to allow restore of earlier versions, for example in the case of a virus attack.
- Consider using a combination of server imaging and granular-level back-up. Imaging is faster when it comes to full server restores, while granular-level back-up enables recovery of small quantities of lost or corrupted data from the remote data vault - even individual files or e-mails.
- Decide what data, if any, needs the added security of replicating the back-up to a second geographical location.

29%
wouldn't consider the cloud due to security fears

53%
only review their disaster plan annually, or less often

It is important to bear in mind the balance between the cost of back-up and disaster recovery arrangements and the probability of any risk crystallising

COST V RISK CONSIDERATIONS

It is also important to bear in mind the balance between the cost of back-up and disaster recovery arrangements and the probability of any particular risk crystallising. The probability of data loss or corruption, or of hardware failure, is relatively high – among the surveyed businesses 26% had had to implement their plan at some point – so it is worth considering a quality cloud-based solution. But you must also define your Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to help determine what solution, at what price, is suited to the individual firm's or company's circumstances. RTO will help balance the cost of any particular disaster recovery solution against the acceptable systems outage time before the disaster starts to negatively impact the business. A shorter recovery timescale usually costs more. RPO refers to potential data loss and is used to determine the frequency of the scheduled back-ups. For example, if you arrange for daily (usually overnight) back-ups, the maximum you could lose is one day's data changes. If that is too much you may select hourly or more frequent back-ups, though that may have cost and systems performance implications.

Most solutions protect only the data and the servers. Arrangements should also be in place to cover the rest of the network and the workplace. Events such as fires, floods and denial of access by public authorities do happen occasionally and a robust and comprehensive disaster recovery solution should also make provisions for full network recovery and for alternative workspace. However, the risk of losing the entire network or use of the workplace is relatively low, so unless the impact of such an event is very significant (for example if you are a bank, a trading floor, an airline) the objective should be to ensure you are adequately covered, but at absolutely minimum cost.

MANAGING UNSTRUCTURED DATA

While fully-automated, high-security cloud-based backup is an excellent solution, the cost is related to the volume of data being backed up. Most organisations are finding it increasingly challenging to manage the accelerating growth of unstructured data. Put simply, data in an accounting system or database is 'structured', while word documents, spreadsheets, emails and so on are 'unstructured' data. This is not just a problem of back-up, however. Managing the technical and financial challenges related to the growth of unstructured data is critical both in the production environment and in the off-site back-up environment. There are cloud-based solutions that can allow the on-site systems to automatically move all unstructured data that has not been used for, say, six months into the cloud (private, high-security), while keeping it available to users if and when needed at the click of a key, as if it were still on-site. This approach can also significantly reduce the cost of off-site security back-ups and dramatically improve the speed of server recovery in a disaster scenario. However, the financial benefits of these solutions kick in only at relatively high volumes of data, so they are not for everyone.

ADDRESSING INADEQUACIES

Disaster recovery arrangements based on tape back-ups, with their well-known reliability issues, and without regular tests of full server and data recovery, are inadequate. A suitable understanding of cloud-based, automated, high-security back-up and disaster recovery can be developed by consulting external experts and by gaining direct experience. This will not only protect the firm, but can also be used to advise clients, with the additional benefits of protecting or even increasing fee income, enhancing client perception of skills within the firm and improving client retention. Furthermore, as technology commoditises and reduces the cost of traditional compliance work, compliance fee income will come under increasing pressure. The ability to offer specialist advice and broaden the firm's skill base will prove essential. Direct experience of back-up and disaster recovery issues is one area of expertise of great value to both firm and client.

26%
of businesses have had to implement a recovery plan

Ian Cockburn ACA MBA
is managing director of Rescue IT

CRITICAL TIME: SYSTEM RECOVERY IN ACTION

A small firm of accountants suffered a major SAN failure at the end of January 2013, which brought their work to a complete halt just before the tax-filing deadline. Fortunately, the firm had signed up to a cloud-based back-up and disaster recovery service just weeks previously.

Working in conjunction with the firm's in-house IT manager and external support engineer, the back-up and disaster recovery service provider established that restoring to the remote standby servers in the data vault would not be the best solution for the client, given that the problem was a SAN failure. Rather, priority should be given to restoring operational capability on the client's own servers, by restoring the cluster domain control servers from the remote data vault to the client's IT environment over the internet.

This restore was completed within four hours and shortly afterwards the client confirmed that they had been able to recover their virtual environment and that their critical servers were fully operational again.

The partner responsible for IT later said the online restore of the DC servers had reduced the time needed to restore full IT functionality by nearly two days, which had been critical to helping them meet the tax filing deadline.