Can you afford the risk?

Ian Cockburn explains why you need a disaster recovery system

An IT disaster may be one of the greatest risks your business faces. They cost money, starting with lost sales and cash flow, and can easily destroy your company. Until recently having a good disaster recovery solution in place was too expensive and too complex for all but the largest businesses. But the needs of SME's have at last been recognised and there are now affordable and easily implemented solutions available.

Three Levels of Risk

IT disasters happen all the time, but most directors are too busy dealing with the day-to-day challenges of running and growing their companies to think about how they would survive a disaster. They may also assume the IT manager, or whoever fills that role, has the risk under control. In reality many IT managers are so busy with day-to-day fire-fighting that they have no opportunity to implement a solution that deals fully with the three cumulative levels of risk every company faces: loss of data, loss of systems and loss of premises.

Risk Level 1 – Loss of Data

Loss of data can be caused by anything from human error, disk crashes, viruses or 'malicious erasure', through to level 2 and 3 disasters. Step one therefore is to protect your data. It is the irreplaceable life-blood of your company. So BACK IT UP! This means having an effective and reliable daily backup routine for your data and system state, with the backup stored securely off-site. It also means doing regular test-restores, to ensure the backups are actually working. Most organisations still rely on tape backups, though these are very vulnerable to human error, not to mention tape deterioration.

Many SME's are now moving to on-line backup services, which are fully automated, securely encrypted, safely stored off-site and immediately available. The cost of such services has reduced significantly over recent years, so this is now an affordable option. It also makes partial or full data restore faster and more manageable.

Risk Levels 2 and 3 – Loss of Systems and Loss of Premises

Fire and theft are the two most common causes of level 2 or 3 disasters, but the risks also include flooding, loss of power or communications, denial of access to the premises – and at the furthest extreme, terrorism.

Even if the building burns to the ground, you need to ensure you can quickly get access to fully operational replacement systems and if necessary, get your 'essential' employees, those

who will keep the business running, immediately re-located to fully-equipped alternative premises. The response must be fast, well-rehearsed and comprehensive. You have to show the outside world and your own staff that it's 'business as usual'.

Very few SME's have the resources or the experience in-house to do all this with the speed and expertise that are required. The answer, especially if you have more than ten employees, is to use the services of a specialist disaster recovery company. The key is to find the right balance between the required recovery window – how long you can survive without your systems – and the cost of the disaster recovery service. This is after all a form of insurance, protecting your company against the terminal effects of something you hope will never happen. The good news is that recently some suppliers have started to offer an insurance-based disaster recovery service at a price every SME can afford. Combined with an effective and totally reliable data backup solution, such disaster recovery services can have your IT systems fully operational, if necessary in fully-equipped, conveniently-located alternative premises, within a timescale that tells everyone it's 'business as usual'. This leaves you and your staff free to concentrate on managing your business and meeting the needs of your customers.

Achieving this peace of mind is no longer complex or expensive. However, managing the risk is the directors' responsibility and does require action – before, rather than after the event.

DTI and other research consistently shows that 70-80% of companies that lose their systems and data never recover; they go out of business within 18 months on average.

Most businesses are increasingly dependent on their systems, not just for 'back-office' functions, but for essential front-line operations and communications. Just think for a moment what capabilities your business could lose if it no longer had the use of its IT systems:

- E-mail communication & transfer of documents
- Order handling, sales management, invoicing
- Collection of receivables and control of cash-flow
- Payment of salaries, commissions, expenses
- Payment of creditors (suppliers, VAT, NI, etc)
- Contact records for customers, suppliers, partners and staff (names and addresses, phone numbers, e-mail addresses)
- E-commerce capability
- Incoming and outgoing web-site access
- Management accounting and reporting

The more fundamental longer-term risks include:

- Damage to reputation and brand
- Damage to staff morale
- Loss of market presence and of customer loyalty & confidence
- Legal and regulatory problems

Clearly, protecting your business against these risks is essential. The challenge is how to do it effectively and affordably.

Ian Cockburn ACA, MBA is Director of RescueIT Ltd. www.rescueit.co.uk

This article will also appear in Business Network, the magazine for members of the Federation of Small Businesses, June/July 2006