



Feature

15 Jan 2009

Disaster recovery

Flirting with disaster

Difficult economic circumstances create their own unique set of threats to businesses, with the increased likelihood that disgruntled former employees could wreak havoc with IT systems - something many business continuity plans fail to plan for, as Jane Bernstein discovers

Studies as well as anecdotal evidence continue to show that small to medium-sized businesses are failing to invest sufficiently in disaster recovery plans for their IT systems and electronic data. This is despite a growing dependence on IT among SMEs. So why are so few protecting their systems should disaster strike and what can the insurance industry do to help?

There has certainly been growing media attention in recent years on the risks posed by viruses and malicious attacks on electronic data. But Tim Dunger, director at Plan B Disaster Recovery, points to a continuing lack of understanding among SMEs about their vulnerability and the difficulties they will face if they need to get their systems up and running.

Asked if the problem lies in a lack of availability of back-up and DR solutions, most industry experts assert that there is in fact a proliferation of such tools on the market. As Ian Harris, senior underwriter for technical lines at Ace UK and Ireland, observes: "There are a number of off the shelf systems from either data security or anti-virus companies and also packages available from service providers such as BT and PC World Business, yet still companies remain vulnerable as take up remains low."

The current economic climate is not helping, of course, as SMEs are increasingly wary of spending money. Shaun Kelly, head of the business solutions group at Crawford & Company for Europe, Middle East and Africa, comments: "I do not see greater engagement by SMEs in the current financial crisis as they tend to regard time and potential cost as a constraint on all aspects of their activity, including business continuity management." He adds that this is perhaps a particularly foolhardy approach in such times as an interruption can have an even more critical impact on the long-term prospects of a business.

Growing concerns

Doug Barnett, head of customer risk management for Axa, points to further recession-related problems ahead: "A massive issue today is staff. You may have a business continuity plan but are the staff that are quoted in that plan actually still there? Many businesses are downsizing now. You may well find that in plans written even just six months ago, there's a good chance things have changed." Mr Barnett also points out that businesses are starting to cut maintenance costs, and may not be replacing outdated equipment. The implication is that as older systems are more likely to go wrong, businesses without a recovery plan are particularly vulnerable.

Traditionally, a lack of awareness of the need for disaster recovery has been blamed for lack of investment on the part of SMEs. But this is no longer widely viewed as a particularly valid excuse. "I am not really sure the problem is a lack of awareness as any prudent business person should always be thinking 'what if something goes wrong?'" says Mr Kelly, adding: "The real issue is perceived complexity around assessing the risks the SME faces, categorising them in terms of likelihood and business impact and responding to them. So the task all too frequently slides down the business agenda and is put off for yet another day."

David Saul, a director at Fusion Internet Solutions, says a "proper understanding of the issues," is one of the major obstacles to SMEs investing in disaster recovery for IT. He observes: "There is no comprehensive view

of what data needs to be backed up, or how frequently. For example, office files, contacts, correspondence and all those 'standards' that are used daily are often not even thought about."

One cause for concern among experts is a lack of testing once business recovery plans are in place. George Quigley, financial services group risk adviser at BDO Stoy Hayward, emphasises: "A business continuity plan that has not been tested simply cannot be relied upon. This stark warning is borne out by the experiences of unlucky businesses who, when using their plan for the first time in a real incident, find flaws and gaps, out of date information and errors. Research has shown that more than two thirds of businesses admit to not having tested their plan."

Mr Quigley adds that a test is often the only way to embed the knowledge contained within the plan into the minds of senior staff. He goes on to explain: "Tests can range from table-top exercises, based in the office, to full 'out on the street' role-play. The most important aspect of a test is to document the lessons learnt, and to make changes to the plan to incorporate these findings."

Another significant problem cited by many industry insiders is a lack of understanding regarding how the IT applications and business processes work. Michael Porteous, senior consultant at Aon Global Risk Consulting, explains: "The fundamental problem for all businesses in designing effective IT risk management and disaster recovery processes is understanding which applications actually run the business and then being able to prioritise and ensure that those critical applications can be rectified and a response process enabled to keep the business running."

Expensive business

Mr Porteous adds that another obstacle is the perceived cost. "The perception is that IT equals expense but that may not be the case. If you really understand your business, it is possible that out of the 300 applications that are running, only five may need to be run on a real-time basis, which would clearly be a less expensive proposition."

There are also some misconceptions around the major threats to IT and electronic data as far as SMEs are concerned. While the threat of floods and fires may keep business owners awake at night, Mr Dunger asserts that these are not the main problems and that in fact the crucial issue is that IT systems inevitably fail. "Computers go wrong," he asserts, adding: "Ask any IT specialist if a computer will go wrong and they will tell you it is not a question of if but when."

So are the available insurance products developing fast enough to cope with the specific problems related to IT disaster recovery and the potential size of the IT related exposures? Mr Porteous believes that the products available tend to be quite broad and do not require the business to demonstrate their effectiveness in managing IT risk in a rigorous manner. "Organisations must be encouraged to have the same level of responsibility for managing their IT as they do for managing their business," he asserts.

The wrong cover

Graeme Newman, business development director at CFC Underwriting, says one of the biggest problems is that while data risks are intangible, most traditional policies effectively cover people for physical damage. He explains: "If you have a fire and it burns down your system then you do have a physical trigger for your business interruption policy. If you have a virus or if an employee maliciously goes in and deletes or damages data, there's no physical damage - and no trigger for your standard commercial policy."

Solutions are, however, beginning to emerge. CFC Underwriting itself offers a stand-alone policy that, says Mr Newman, means it can cover SMEs and larger companies for a virus incident, hacking attack or the actions of malicious employees. Ace also has a number of solutions. Specifically, its Computerguard Plus product protects the insured's computer equipment and also their data from malicious attacks whether they come from outside or inside the business.

Malicious attacks are, in fact, a growing problem for SMEs. As Mr Harris observes: "Many companies still do not immediately rescind employee access to their systems and as such they remain vulnerable to virus attacks, time bombs or any other sort of malicious act by people able to enter into and access all their systems. Companies seem to be unaware that the majority of specific attacks on IT systems tend to be from disgruntled current or ex-employees rather than random attacks by disinterested parties."

John Hagger, an associate director in the risk management placement practice at Marsh, recognises that there are insurers out there who have developed niche products. He says the issues clients consider will centre on

whether they will pay for this kind of niche product or whether they see such risks as day-to-day operational trade risks that they can risk manage internally or with the aid of external risk consultants. He adds: "That's the challenge for any insurer that chooses to offer this. If they are going to commit to the research and development to produce a new product, they have to be confident that there is a market for it."

Providing cover

The insurance industry's involvement in business recovery planning is not limited to providing cover. Brokers and insurers also have an important role to play in terms of incentivising businesses and providing risk management advice. Aon, in fact, is developing an IT risk management process that Mr Porteous says aims to "help clients to identify and understand their IT risk profile and seek the most cost effective risk financing solution. Insurance may be one mechanism that can be used to transfer some or all of this risk." Mr Porteous points out that once an SME has a plan that has been tried and tested, the broker can then present this to the underwriter. "The underwriter is then given an increased level of assurance that the impact they may experience as a result of an interruption in terms of payout is going to be significantly reduced."

Of course, the implementation of DR plans in no way guarantees lower premiums. Mr Hagger observes that any reduction in premiums will depend on a wide variety of factors such as the quality of information presented to insurers to enable them to evaluate or validate those plans and that this is especially pertinent on new prospects.

Mr Dunger points out that the provision of risk management advice can be an important differentiator for brokers in terms of the service they offer. He explains: "Brokers, underwriters and insurers are really starting to look for things that will broaden their horizons with the client - and differentiate their service. Advising on disaster recovery should be a part of that. If brokers can demonstrate a high level of ability and professionalism by advising on IT risk management, and therefore do their job more 'in the round', they can only profit."

There is little doubt that SMEs, along with larger businesses, will become increasingly dependant on IT and electronic data. And it appears that many still need all the help they can get to protect these vital systems. It is also clear that insurers and brokers can play a significant part in assisting their SME clients on crucial disaster recovery planning.

DISASTER RECOVERY: KEY STEPS

To protect their business, most organisations will have to ensure they have a practical effective plan for recovering their IT systems as part of an overall business continuity plan. Here are a number of issues that should be considered:

1. Do have a plan. Follow best practice for business continuity planning and plan for the small as well as the big disasters.
2. At the very least take back-ups of all systems. However, it could take three to five days to buy a new server and recover the back-up data. If there are multiple inter-dependent systems, the challenge is even bigger.
3. Decide exactly which systems are critical to the business and how long the business could do without them before suffering irreparable damage.
4. Choose a disaster recovery provision that will work (many don't stand a chance of working in an actual disaster), and that will get back working systems in the state they are needed before the business is ruined.
5. Choose a disaster recovery provision that is continually tested and can be proven to work in the way the business needs it to.
6. Beware of any arrangement that relies on intermittent human tasks. They are bound to get forgotten or prioritised out of the task list, and you won't realise until you need it and it doesn't work.
7. Make sure staff know the plan and can implement it under pressure.
8. Test the entire plan at least once a year. Test for the worst situation.
9. Revisit the plan regularly and adjust as you learn.

10. Check the IT disaster recovery plan is not completely dependent on all or any particular members of the IT team. Sod's law will ensure they are on holiday when disaster strikes or worse they are caught up in it. Source: Plan B Disaster Recovery.