Bouncing back

Executive summary

- **Companies need to establish that they have the ability to protect against system downtime by installing a secondary system so operations can continue and they do not lose the most critical asset of all: information.**

Recent years have provided graphic examples of how unforeseen events can suddenly disrupt business activities and operations. A period of no more than two years, from mid-2005 to mid-2007, was marked by the 7 July bomb attacks in London, the Buncefield oil depot explosion, the most widespread flooding for years and interruptions to power supplies. More recently, even central London has been hit; in late April, a burst water main caused extensive damage at City Hall and forced nearby businesses to temporarily relocate.

SURVEY FINDINGS While damaged premises and denial of access for employees can bring businesses grinding to a halt, for many companies, protecting information technology has become the priority as an integral part of their overall business continuity strategy.

According to the recently published 2008 *Information Security Breaches Survey*, carried out by a consortium headed by PricewaterhouseCoopers, 58% of respondent companies said they would suffer significant disruption if their information technology system were unavailable for a day. The percentage rose to 70% for large companies.

Nearly all of the companies that participated in the survey said they took the precaution of backing up their critical systems and data, with 86% doing so on at least a daily basis.

The survey also suggested that the percentage of UK companies with a disaster recovery plan in place has risen, from 58% in 2006 to 72% today. For the largest companies, the figure increases to 91%.

However, some of the survey's other findings were less reassuring. More than one in four of the respondents said they had no disaster recovery plan in place. Nearly half of those that did have a plan in place admitted that they hadn't actually tested its resilience within the past year. And while more than nine out of 10 businesses said they considered disaster recovery to be an important driver of their IT expenditure, 15% did not take their backups off-site.

Possibly as a result of local businesses suffering disruption during last summer's floods, south-west England has overtaken London as the region with the most disaster recovery plans in place, although the region came out no better than others when it came to actually putting those plans to the test.

ESTABLISHING A CONTINUITY PLAN A business continuity plan defines how a company will respond to disruption. Disaster recovery is that part of the business continuity plan applying specifically to maintaining IT systems. Both need to be linked. "Your disaster recovery can be fantastic, but if you haven't also got a comprehensive business continuity plan in place, then it's a pointless exercise," says Guy Bunker, Chief Scientist for Symantec Corporation.

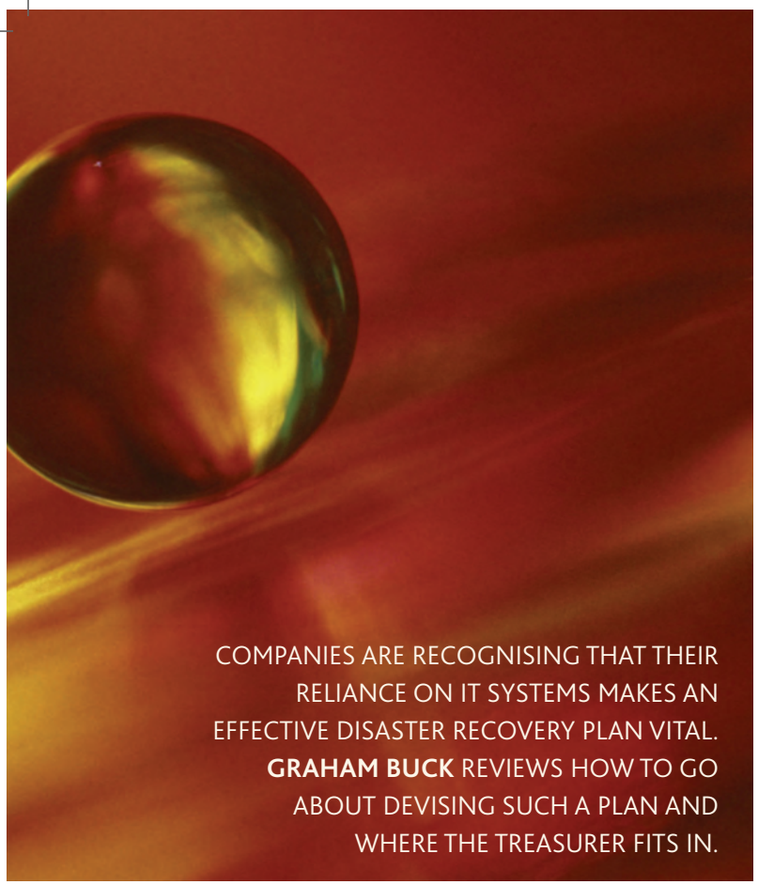
Devising both plans should involve senior management including the chief executive, although Symantec's research indicates that this is not yet the case for many companies. However, corporate chief information officers now typically have a seat on the board in recognition of how important to the business the smooth running of IT has become.

Another obstacle is that IT is an expensive buy and a comprehensive disaster recovery plan does not come cheaply. Many of the companies surveyed by Symantec cited limited resources – principally, budget – for either the lack of a disaster recovery plan or one that was relatively basic.

According to Dave Gilpin, Products and Solutions Director for business continuity specialist SunGard Availability Services, the increased focus on disaster recovery has been a "slow burn", with no sudden advances. Instead, it has steadily developed into a mature market through a combination of more demanding regulation, advances in technology, competitive practice, benchmarking and education. "Add to these events such as Buncefield, which motivate people to ask 'What exactly would happen to us in the same circumstances?' There has always been a degree of pressure from the regulatory authorities, and the major financial institutions have been involved in London-based tests and trials co-ordinated by the Bank of England. Although smaller companies face similar requirements from the Financial Services Authority, they are implemented slightly more loosely."

HARDWARE FAILURES STILL TOP THE LIST The development of instantaneous trading since the 1990s has pushed disaster recovery higher in the corporate agenda, not only for financial institutions but also for major commercial organisations such as Tesco, which now keeps a watch electronically on warehouse stock levels.

SunGard's own records on the major causes of business disruption



COMPANIES ARE RECOGNISING THAT THEIR RELIANCE ON IT SYSTEMS MAKES AN EFFECTIVE DISASTER RECOVERY PLAN VITAL. **GRAHAM BUCK** REVIEWS HOW TO GO ABOUT DEVISING SUCH A PLAN AND WHERE THE TREASURER FITS IN.

Questions for a disaster recovery strategy

FIRST STAGE

- Where does information enter the organisation?
- How is it processed?
- How is it stored?
- How is it accessed, and by whom?
- How is it used?
- Who owns the information?

SECOND STAGE

(A company proceeds to this stage only after the information flow has been understood and mapped)

- What are the risks to the information flow?
- What external and internal dependencies exist?
- What safeguards need to be put into place to ensure that information is always available?

Source: SunGard Availability Service's report *From Adversity to Availability*

show that hardware failures are the biggest single cause of customer invocations (where one of its clients declares a disaster requiring its services). Its top three over the past two years are:

	2007	2006
Hardware failures	35%	45%
Power-related disruptions	22%	31%
Flooding	12%	6%

Last summer's floods in the UK resulted in a large jump in denial of access situations; companies avoided flood damage to their own premises but suffered the consequences of other properties in the vicinity being affected and the surrounding areas being cordoned off.

To be effective, a disaster recovery plan should adapt to a variety of events that could interrupt a company's IT applications. They range from those that threaten long-term disturbance, such as a Buncefield-type incident or a terrorist attack, to those likely to prove only transient, such as a power outage.

A company's attitude can range from "going bare" on disaster recovery, or having only the most basic system of backup tapes for non-critical applications from which information can be recovered, to the very highest level of sophistication, where if a system goes down another can take over within minutes.

Recent surveys suggest that companies' main concerns over the impact of unexpected disasters are damage to their brand and reputation, the effect on customer loyalty, the impact on their competitive standing and the potential repercussions from loss of company data. Treasurers have the task of weighing up the risk and the cost benefits, including the ongoing costs, of any disaster recovery exercise.

SECONDARY SYSTEMS ARE CRITICAL A disaster recovery plan identifies those applications most critical to the company and the hardware on which they run. Email, for example, is one application that has moved from being "a second-tier application to a first-tier," says Bunker.

The next stage involves devising a recovery plan appropriate to various events. For a financial institution, which can lose substantial amounts if a system is down for even an hour, this involves a backup system that can respond immediately to any interruption.

The popularity of online banking makes it vital to have a secondary system that can be up and running quickly. An illustration of this is provided by Northern Rock; the lengthy queues that built up outside the mortgage bank's branches last September when its problems became public were due partly to the unavailability of the website, which crashed under the unusually heavy volume of user traffic. A secondary system has become equally essential for businesses heavily or wholly reliant on web transactions, such as Amazon.

Some systems require duplicate hardware on a different site, where staff must be retained to maintain and test it. Although it is possible to limit the test to parts of the system only, a full test is periodically required to identify the weakest links, says Guy Bunker.

"Many companies wait until the weekend to conduct large-scale disaster recovery tests," he says. "Fewer people are there and the test can get under way at, say, 8pm on Friday evening. It's also a safeguard against it taking longer than anticipated to get the system back to normal; for example, because the configurations have changed."

BOARDROOM HOT TOPIC Despite survey findings that suggest chief executives still have yet to get directly involved, disaster recovery has moved up the boardroom agenda. As the duties and responsibilities of directors have increased and been outlined in codes of good corporate governance, so a robust disaster recovery plan has become an important component of good corporate governance.

However, while disaster recover has become a boardroom issue, many directors assume that business interruption insurance will be enough to meet all corporate needs in the event of disaster. However, as SunGard observes, "Insurance provides no protection; it only offers compensation." Companies can obtain expert advice in recovering their infrastructure and premises in the event of disaster, but that will not allow them to continue operating throughout a disaster. Nor will they be protected against system downtime or properly recompensed for the loss of their most critical asset: information.

Graham Buck is a Reporter on *The Treasurer*.
editor@treasurers.org