

Cost-cutting and complex IT raise risk of disruption

Print

By Stephen Pritchard

Published: April 21 2009 16:31 | Last updated: April 21 2009 16:31

Agrowing crisis is threatening ever more businesses, as figures show that last year, 40 per cent of UK organisations faced business disruption as a result of an IT failure.

Worryingly, research carried out by the UK government's cabinet office and the Chartered Management Institute shows the dangers are increasing significantly: in 2002, just 19 per cent of organisations faced similar problems.

The UK is just one example of this trend: throughout advanced economies, the number of IT-related interruptions has grown steadily.

But the current economic environment is affecting organisations' business continuity plans in different ways. Some companies, for example, have increased spending on resilience, as any disruption might mean a permanent loss of profits.

"IT managers are being forced by the business to ensure that resilience is built into projects. If a system is coming in, it will be classified as critical and will require high availability," says Bill Broadley, principal consultant at business and technology consultancy Morse. "Most IT providers and IT organisations in banks will have resilience high on the agenda... IT directors are being told that they cannot afford any downtime."

But other organisations have actually cut business continuity spending, along with other areas that might lead to disruption, such as IT security, or systems maintenance.

Added to this, continuity plans designed and tested in more buoyant times could now be harder to implement, because key staff have left. Job cuts mean there are not enough people available to maintain all business processes after an incident, and not just in IT.

"There may well be a higher likelihood of something going wrong and the impact of an outage may be more damaging, because organisations no longer have the right people in place," cautions Roberta Witty, research vice-president at industry analyst Gartner. "An outage could have a bigger impact [now] than even last summer."

Another factor is that some organisations let investment in continuity fall, even before the economic downturn. In others, spending on resilience has not kept pace with the increasing complexity of IT systems.

"In some respects, we have gone backwards when it comes to business continuity," says Rick Cudworth, head of business continuity and resilience at Deloitte, the professional services firm. "It is partially due to under-investment and partially the increased complexity of IT. Many organisations are not in as good a position [to recover from an incident] as they were five or 10 years ago."

Some IT systems are now so complex that chief information officers responsible for them doubt that they could recover in time from a total loss – such as the destruction of a building or datacentre – to save the business, even if the data itself were fully protected off site. Large banks and government organisations have fully replicated systems, but elsewhere the emphasis has moved from recovery to avoiding failures in the first place.

"IT is massively more complex. We have more servers, and more applications that are classed as 'tier one'," says Richard McGrail, head of IT at Baillie Gifford, an investment firm based in Edinburgh, Scotland.

"The reason we provide replication and incremental back-ups is in case something happens to our building. But the secondary issue is that the safety net is now so complex, it can cause the very problems we are seeking to avoid."

As a result, organisations such as Baillie Gifford deploy what Gartner calls a "layered approach" to business continuity and resilience. The firm uses both a business continuity facility, provided by vendor Sungard, and a Citrix remote environment that allows its investment professionals to work from home.

In addition, critical information feeds are located through a "neutral" venue so they can supply data to staff at either the main office or the continuity site.

The company's plan is based around preventing outages and a disruption to trading, Mr McGrail says. "It is about reputational damage, but the biggest fear for us would be if we lost trading data... reproducing those sequenced trades would be an operational nightmare. It would distract the company terribly, and that would expose us to even greater risks, as people would effectively be trying to do two jobs."

But it is not just the complexity of IT systems, but their importance to the business, that should be forcing boards to look again at how they protect their key systems. In environments where reverting to manual back-ups is hardly an option, business continuity is giving way to the notion of business resilience.

Organisations need to be built to withstand shocks and disruption, and IT systems should reflect this. If budgets are tight, companies might face the stark choice of either building a resilient system, or having a well-resourced

and tested continuity and recovery plan.

“You need both, but if I had to make the choice I would rather have resilience,” says Paul Kirvan, a US-based business continuity expert and a board member of the Business Continuity Institute. “It is very difficult to get people to make and test a business continuity plan. It is less difficult to build resilience into the hardware, software and network. If I had \$500,000 to invest in IT infrastructure, one area I would be looking to improve is the resilience and survivability of some of my key assets.”

Business continuity experts stress that prevention is better than cure, as even the best plans can be overtaken by events. More importantly, any recovery plan takes time to implement. That is time when the business will not be able to trade, and will lose revenues.

“Even if you can recover successfully, there is always an impact,” says Stuart Anderson, a business continuity expert at PA Consulting. “We are now talking about business resilience and building in that resilience, rather than business continuity planning, or planning to fail. That has had its day.”

Instead, companies should be looking at whether their operations can be split or dispersed, and how workloads can be spread between sites, both during day-to-day business or during an emergency.

Although companies looking to save costs might be tempted to reduce their number of operational sites, Mr Anderson points out that public sector organisations are increasingly looking at dispersal as a way to “harden” their operations and services against disruption. “The technology is there, but cultural and business change is also needed if you want to make the organisation more resilient,” he cautions. “It is not just an IT issue.”

To cope with this, organisations need to have plans that will allow for a staged “invocation” of the continuity plan.

A degradation matrix will set out which services need to be recovered and which can be allowed to deteriorate, or even fail.

During a short-term outage, such as bad weather, home working might be an option for some employees. But longer-term disruption would need more comprehensive measures, such as the move to a back-up site. For more disruptive incidents, factors ranging from morale to the availability of public transport, catering and even janitorial services will all need to be part of the plan, according to Mr Anderson.

“Businesses are planning for more, not less, uncertainty,” he says. “Unexpected events are likely to increase, so it is also about the resilience of your brand, your marketplace and ultimately, the resilience of your investors.”

[Copyright](#) The Financial Times Limited 2009