June 2012

Enterprisewide Business Continuity

When planning to ensure continual availability of critical business functions, organizational considerations need to extend beyond the IT department.

Neil Baker

In June 2005 New Zealand's entire telecommunications network failed. A break in a cable on the country's North Island led to services being routed to a different part of the network, as dictated by a national disaster recovery plan. But at exactly that moment, a Telecom New Zealand worker damaged a second main line in another part of the country, resulting in a nationwide outage. And the cause of the initial failure? A rat had chewed through a cable.

The combined actions of one careless worker and one rodent forced the New Zealand Stock Exchange to stop trading. The damage to business more widely was significant. But this was seven years ago — imagine what the impact would be today, when so much business activity depends on the Internet and other networks. Look at the effect a technology failure had on Research in Motion, the company behind BlackBerry devices. Last year, a sustained service outage across large parts of the world left millions of customers without email for days, inflicting considerable brand damage.

Organizations are more dependent on IT than ever before, but IT failure is just one source of potential disaster. From the BP oil spill and Hurricane Katrina in the United States to the tsunamis in Japan, crises of enormous proportions may strike at any time and have devastating effects. Even a mundane failure — maybe just a burst water main — can bring an organization to its knees. Continuity plans need to deal with these threats, too. But it's often IT concerns that dominate.

Internal auditors are in an excellent position to help redress the balance. They should have the knowledge, skills, and profile in the organization to encourage a more enterprisewide approach to continuity planning. But it's not easy. Getting senior executives to recognize the need for more holistic plans is one thing, but getting them to do something about it can be another challenge entirely.

Continued…

NOT JUST AN IT ISSUE

It's no surprise that technology concerns tend to dominate continuity planning, says Phil Samson, leader of PricewaterhouseCoopers' U.S. business continuity service, based in Dallas. From the earliest days of modern computing — via mainframes, data centers, and now cloud services — the need for backup plans in case of disaster has been well understood.

Moreover, the technology function is a discrete unit inside most organizations. "It has a leader, someone who says 'I am responsible for keeping the technology up and running,'" Samson says. That clarity of risk ownership makes it easier for the IT leader to muster the resources needed to put in place technology resilience and recovery programs. "It's their money, and they know what needs to happen," he says.

But move recovery planning out of the IT arena — to human resources, regulatory compliance, or supply chain resilience, for example — and that sense of ownership soon decays, he says. And with it goes the quality of planning.

Yet over the last five years the situation has been improving, says Alan Berman, president of New York-based DRI International, a nonprofit that certifies business continuity professionals. More companies have begun to take a wider view of continuity planning, looking beyond the threats to their IT systems.

The reason, he says, is the rise of other business-crippling risks that are just too big for management to ignore. Terrorist attacks, pandemic threats — such as the SARS virus and avian flu outbreaks — and a succession of natural disasters have made it clear that keeping technology up and running is just one priority. There's little comfort in knowing that your data center or office networks are available in a crisis, if your staff can't travel to work or are in bed sick.

Regulators across different industries have received the message, too, Berman says. The financial services sector has always had a strict approach to business continuity planning, for obvious reasons — if a bank went down, it would cause chaos. Continuity planning also has a high profile in infrastructure sectors such as energy, water supply, and transport. But here, too, the emphasis now is on dealing with wider issues of business resilience, rather than just IT recovery, Berman says.

Even in less regulated sectors, companies are becoming more aware of the need for enterprisewide continuity planning. Supply chain concerns are a particularly hot issue, Samson says. The tough global economy has accelerated the trend for companies to cut costs and free up working capital by making their supply chains leaner and more efficient. Just-in-time ordering and delivery has cut inventory to the bone, and many companies have slashed the number of suppliers they deal with. While improving efficiency, such steps can make supply chains dangerously fragile.

The massive flooding in Thailand last year is a case in point. Japanese carmakers with component manufacturers and assembly plants in the country lost 6,000 units of production daily at one point, according to the Japan Automobile Manufacturers Association. The disaster cost the top three automakers more than US $500 million a month, according to JPMorgan Chase & Co. The flooding also hit Western Digital, the world's largest maker of hard-disk drives, which posted a quarterly loss and said production wouldn't return to normal for months.

Continued…

ASSESSING CONTINUITY RISK

While some companies are only now understanding the need to take a more holistic view of business continuity, the internal audit profession has recognized the importance of keeping threats to IT in context for a while, Samson says. An essential resource for companies wanting to raise their game in this area is The IIA's *GTAG 10: Business Continuity Management*, published in 2008, he says.

The guide draws some practical distinctions among disaster recovery (which is focused on IT), business continuity management (the process of developing and testing enterprisewide plans), and crisis management (how those plans are deployed, if needed). It also provides advice on how an internal audit shop can assess an organization's capabilities in business continuity management (BCM), explains the different parts of a comprehensive continuity program, and shares ideas on how to make sure they are in place.

But the guide's introduction includes an observation that is likely to be depressingly familiar to many auditors: "Whether due to economic downturns in an industry, lack of informed management, or other corporate cost decisions, BCM program champions such as chief audit executives (CAEs) often find their recommendations to executive management for improved BCM to be ignored or deferred far into the future." The bottom line, according to the guide, is that the CAE should be able to answer "yes" to three simple but important questions about business continuity (a "no" to any is evidence of a problem):

> Does the organization's leadership understand the current business continuity risk level and the potential impacts of likely degrees of loss?
> Can the organization prove the business continuity risks are mitigated to an approved acceptable level and are recertified periodically?
> If an unacceptable business continuity risk exists but executive management has decided to assume the risk, are the organization's owners, business partners, and other constituents aware that management has decided not to mitigate the risk? Also, has the decision to accept the risk been documented correctly?

The key to getting companies to take a more enterprisewide view of business continuity is the same as it would be for any important change program — get senior executive buy-in, says David Everest, one of the IIA guide's joint authors and an information security specialist at Cleveland-based KeyBank, a financial firm.

His advice is to put the spotlight on business processes, not IT systems — show executives how much money the organization could lose if the process fell down. "Lost revenue is what's going to drive the recovery effort," he says.

Samson says that any crisis will hit an organization in one or more of just four areas: loss of technology, people, facilities, or critical third parties. "If you show executives the impact on those four areas — whether you are talking financial, reputational, regulatory, or other impact — that will show you the processes that need to be up and running, and in what order, and who the owner of each process is."

Kelley Okolita, a consultant in this area and author of Building an Enterprise-wide Business Continuity Program, stresses the need to engage management with disaster scenarios that it believes to be both credible and — with planning — survivable. "Nobody believes in 'The Big One,' they just can't get their arms around the idea of a catastrophe," she says.

Continued…

However, the sense of imminent threat is an important motivator for change. "My job is to scare people so that they take action," Okolita says. And she can quickly point to several truly alarming scenarios — for example, data showing that the U.S. Pacific Northwest is overdue for a massive earthquake.

But Okolita notes that most disasters that disrupt business activities are not what she calls "smoke and rubble events." One financial firm she worked for had its head office shut down because a water main along the street burst —"They don't let you stay in a building with 1,600 people and no flushing toilets," she says.

When Okolita works with a new organization, she is quick to drop by the internal audit shop. She often tells auditors that they are asking the wrong questions about continuity planning. A typical audit checklist may look at the quality of the plan in place, whether it has been tested, when it was last updated, and whether it covers certain scenarios, she says, "but the right question to ask is this: Is your business recoverable?" In her experience, many organizations have invested millions of dollars in continuity plans that just don't work because that basic question was never asked.

Samson also encounters audit shops that need to change the way they think about continuity planning. The GTAG guidance does a good job of showing internal auditors the kind of red flag planning weaknesses they should look for (it includes a sample audit guide and a BCM capability maturity model), "but what tends to happen is internal audit will often look at BCM and come up with a standard set of recommendations," he says.

Common findings, he says, are: The IT department's recovery plans do not match what the business needs; business users are not involved in testing the plan; and the plans, if they exist, don't reflect changes in the organization, such as new acquisitions or decisions to outsource services.

To move toward a more enterprisewide approach to BCM, organizations must carry out a more rigorous business impact analysis, Samson says. "And if the company has not taken that first step, internal audit should think about doing it, or sponsoring it," he says. "Because without it, the rest of the BCM program just won't work — there won't be any perceived need for it."

HOLISTIC ASSESSMENT IN PRACTICE

At Dyson, a British company that makes consumer appliances, Dan Harvey, head of internal audit and risk, is working to implement a more holistic approach to business continuity. "Historically, continuity planning has been done by operational management," he says. "While this has been successful in some areas, the varying risk appetites of departments have led to inconsistency across the organization. This year business continuity management has come under my remit—my team will identify and communicate board-level risk appetite, and ensure a common approach to risk identification and mitigation."

Parts of the company — particularly IT — have a better understanding of continuity planning than others, he says. "The path of least resistance would be to focus effort on these functions, but by spending your money on technical solutions you don't achieve the business resilience you really need in the case of disaster."

Continued…

The company sources components from around the world, so supply chain risk is a high priority. "If we were just to focus on IT, this critical area would be missed," Harvey says. "We are currently looking to get a better understanding of our manufacturing supply base — not just our primary manufacturing partners but also secondary, and in some cases tertiary, tier. We want to really understand what might cause supply interruption, what that would mean to our business, and therefore what we could and should do about it. There is no capital outlay necessary for this, but we will be mitigating one of our key potential exposures."

Harvey's advice for other audit functions wanting to improve their organization's approach in this area is to engage with business management from the outset and understand the commercial impact of continuity failures. "Be realistic and pragmatic about the likelihood and impact of disaster," he says. "Accept that continuity will rarely be a No. 1 priority for operational management, but if you can communicate its value and demonstrate how it can bring commercial as well as resilience benefits, you will get buy-in and make real progress."

In that sense, enterprisewide business continuity isn't just about putting in place better plans so that the organization has a greater chance of withstanding a crisis. It's about understanding the business better — knowing where the risks are, what impact they might have, and whether enough is being done to mitigate them. It dovetails perfectly with enterprise risk management and should be a high priority for every internal audit shop.

Neil Baker is a freelance writer who specializes in corporate governance, internal audit, and risk management issues.