

# The fifth in a six-part series on Corporate Risk Mitigation looks at the importance of preparing for external risks and containing crises



## Putting a lid on calamity

**F**or reasons we can all understand, much of the corporate world's collective attention in the past 12 months has been on the containment or mitigation of further financial risk. That clearly makes sense, but as news reports remind us every day, companies

face a whole host of other risks – some foreseeable, others striking more or less out of the blue – which can damage, disrupt or completely debilitate a business. Depending on the location and type of industry, these can range from natural hazards including fire, flood, earthquake and typhoon to “man-made” crises, which stretch across the spectrum from arson and acts of terror to industrial sabotage or events precipitated by a change of political regime.

As if that wasn't enough, a third category of external risks is also ever-present and demanding ever more attention. Broadly speaking, it covers all those potential problems linked to health matters or environmental factors. One year, for example, a company may find itself contending with the effects of Sars or swine flu; the next, it may be having to clean up a chemical spill or explain itself in the court of public opinion for creating pollution or appearing to condone environmentally destructive practices.

Surprisingly often, senior executives caught up in these types of incidents seem to believe the first and best line of defence is to claim that “no one could have seen it coming”, or that what happened was beyond anyone's control. In certain cases that really is true, with the Indian Ocean tsunami of late 2004 being one of the more dramatic recent instances of disaster striking out of nowhere. But much of the time, the risks that businesses face, however extreme or unlikely they may be painted, are foreseeable. Japan is in an earthquake zone, faulty wiring can spark an all-consuming factory fire, computer systems malfunction, and a flu epidemic at home or in overseas markets can quickly erode revenues.

Therefore, a key aspect of every manager's responsibilities must be to anticipate worst-case scenarios. It is also essential to think through the various likely consequences and to put in place plans to avert them and, should

### EXECUTIVE INSIGHTS

Edited by John Cremer

Staff need to know that the first 48 hours are the most critical in handling any emergency

that prove impossible, contingencies to contain the most damaging effects.

Unfortunately, what we see in our capacity as consultants is that many organisations are ill-prepared to deal with major crises. They allow foreseeable risks to go unmonitored or disregarded and, as a result, fail to take the preventative measures that can minimise later fallout. Therefore, we generally start by reminding people of the old military adage that time spent in reconnaissance is seldom wasted. In practical terms that usually means addressing a series of “what-if” questions and getting senior executives, managers and department heads to consider what they would or could do in certain challenging situations.

Initial examples would relate to the sort of everyday scenarios any well-run company should already have thought through in detail. They could include large-scale staff defections, the loss of a major client or key supplier, aggressive pricing tactics by a competitor or labour unrest. From there, though, it is important to go a good deal further, stretching the imagination to contemplate possibilities which, in the regular course of events, might seem well beyond the norm, but could still happen.

A good starting point for such an exercise is to consider a few headlines from stories reported the previous week. And the next step is simply to ask all the “what-if” questions that would logically follow if your own company found itself affected directly or indirectly by a similar situation. Doing this, those involved in

the session might have to consider how to react if, for instance, a major supplier was indicted for corruption; a top executive was caught in a terrorist attack; a flood suspended all production in Bangladesh; or a new computer virus attacked a key database.

The objective, of course, is not just to mull over such problems from a hypothetical point of view. It is to come up with concrete action plans that could be implemented if the need ever arose. And while some might query the need, such exercises should be thought of in the same way as standard fire drills, or earthquake drills in Japan, vital for guarding against risk and potentially crucial for protecting staff and sustaining the business.

While no list can be exhaustive, we have found that certain areas of corporate operations merit special attention and contingency plans. These include:

**Systems back-up** To ensure procedures and hardware are in place to store critical data in a secure separate site.

**Viable alternative suppliers** No matter how reliable or cost competitive certain suppliers may be, it never makes sense to put too many eggs in one basket.

**Locations** In case something catastrophic happens, there should be provisional arrangements for key staff to continue working from home or another designated office.

**Insurance** It is important to review policies regularly and, if necessary, amend them to take account of changing risks and new threats to the business.

**Health measures** Lessons learned from the Sars outbreak and other flu epidemics should lead every company to have its own rulebook to prevent the spread of disease, maintain hygiene, and enable operations to continue with a skeleton staff.

Larger companies often use risk registers to identify possible problem areas in their organisations. These are helpful but not infallible, since the key in any such process is to develop realistic plans that will work in context and in practice when the worst actually happens.

That entails keeping staff generally informed and training those required to handle special duties as part of a designated crisis containment team. They need to know that the

first 48 hours are the most critical in handling any emergency. To be effective, there must therefore be a clear chain of command, definite procedures and no room for equivocation.

The size and composition of a crisis containment team will obviously vary depending on the scope of the company, the industry and the geographical spread. In general, though, the team should include representatives from senior management, finance, operations and the legal department. It may also make sense to draft in external consultants to give advice on the outline plans, as well as on handling crisis communications. This is a very specific skill, quite different from run-of-the-mill PR assignments or standard press announcements.

The collective goal should be to facilitate well-informed decisions and implement them quickly and consistently. Crises come in all shapes and sizes, but the most effective responses all tend to follow a classic pattern. That depends on doing a fast and comprehensive assessment of the incident, its immediate impact and likely future damage, and then activating contingency plans without delay. There are no prizes for holding back or postponing decisions. The whole point is to move with speed and decisiveness.

As the situation evolves, members of the crisis containment team should never just rely on whatever procedures were drawn up in advance. They must also be ready to improvise, constantly reviewing developments and redirecting their efforts as they see what works and what doesn't, where special attention is needed and what can look after itself.

By their very nature, crises are unpredictable. However, with a well-thought-out plan in place, companies can avoid risk or mitigate damage to their business, their reputations and the broader community.

Article contributed by Steve Vickers, president and chief executive of FTI-International Risk, a leading risk mitigation consulting and investigative organisation in Asia