# To be PREPARED is HALF THE VICTORY

In this How to… guide, Chris Paton highlights the six core principles of good – and well-managed – disaster recovery, regardless of the type of business emergency encountered

I have recently read the business contingency article on S.P. Richards (SPR) and the company's recovery from a devastating fire in the last issue of **OPI** *(see Special Feature,* ***OPI*** *December/January 2020, page 24)*. I found it very interesting for a variety of reasons. The honesty of those being interviewed stood out in particular – being willing to openly discuss what had gone well, alongside what had gone on their 'ugly' list was refreshing.

The article really helped to highlight some key learnings which I would suggest match the six principles that I consider to be essential in any type of disaster recovery. As the headline – and indeed many centuries ago Spanish novelist Miguel de Cervantes – says: "To be prepared is half the victory."

### 1. Have an early warning system

It seems obvious, but the best means of business contingency is to avoid the crisis in the first place. To do that requires good foresight, based on sound data, yet it is surprising how few organisations have a specific team scanning for vulnerabilities.

These teams should be looking at specific current threats, but also at trends. This allows leaders to consider potential issues well in advance and implement preventative measures that mitigate the risk ahead of time.

Even if threats aren't increasing, risk teams should conduct tabletop discussions on where the organisation is currently more vulnerable than advisable – such as an over-reliance on a particular distribution centre or IT structure.

### 2. Keep agile

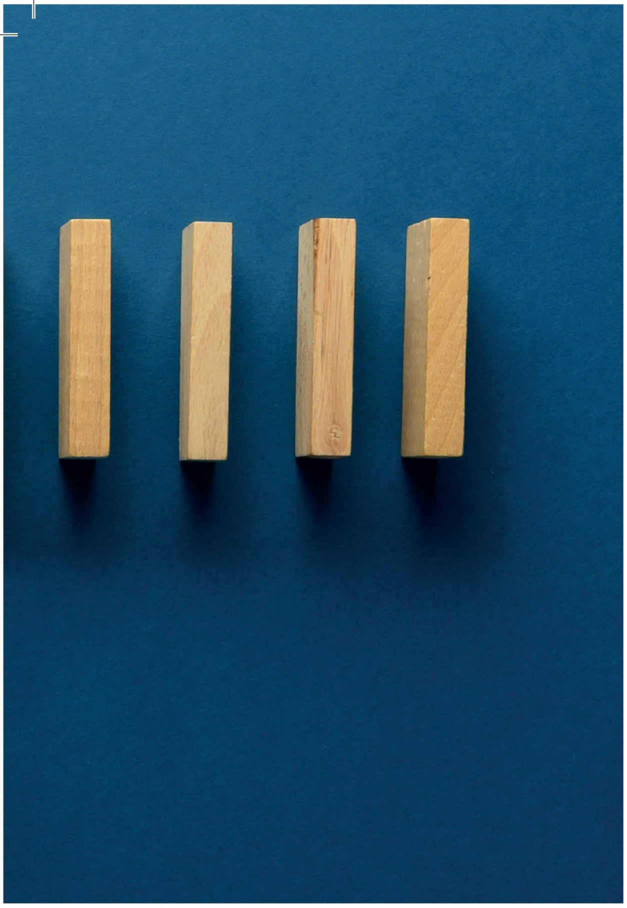
A business can be hit from many different angles – cyberattack, fire, flood or even a severe outbreak of illness, as well as wider incidents such as public demonstrations/riots, terrorist attacks, or regional conflicts/wars.

The answer to this is usually 'focus on the most likely' and generate detailed response plans for them. Sadly, it is invariably the one thing you haven't prepared for which is the one that will happen for real. As such, a far better approach in my view is to have a well-rehearsed process that kicks in regardless of the situation, yet has flexibility of decision-making and adaptation built in. This is exactly how SPR appears to have managed a difficult situation – the basic processes were in place and they were adapted on the fly. The wholesaler wasn't rigid in its approach or tied to a process that wasn't working.

### 3. Don't rely on key individuals

If your recovery plan is purely based on some key individuals with specific skill sets, you are heading for a problem. You can bet that they will be away from the office at the crucial moment or out of communications.

It's more useful to have a plan that is known across the organisation and which can be implemented by anyone and is accessible from anywhere. There are lots of good tools available to help with this approach; my personal favourite is Method Grid, a cloud-based solution which



*Chris Paton is Managing Director of Quirk Solutions, a management consultancy specialising in business resilience and execution success which works with large brands such as Unilever, Lloyd's Corporation, Shell, Heineken, John Lewis Partnership and Linklaters, as well as SMEs and public sector entities including the NHS and the Home Office. In his former career, Paton was a Lieutenant Colonel in the Royal Marines and advisor to the UK government's Cabinet and National Security Council on the Afghan strategy.*

allows you to set out a step-by-step process but also build in checklists, videos, top tips, emergency contact details etc, so that anyone can manage the plan, from anywhere.

### 4. Challenge the status quo

I often see businesses conduct continuity exercises. Carefully scripted, these run through a series of dilemmas to test the readiness of the teams to react in accordance with the recovery plan. But what if the recovery plan doesn't reflect the current threats? When do we challenge if the plan or its processes make sense?

> "It's more useful to have a plan that is known across the organisation and which can be implemented by anyone and is accessible from anywhere"

I recommend a test, reflect, learn approach instead. Run through a scenario for a short while, then take an immediate pause to talk through what happened. Who took the decisions? When? How? Via what communication channel? On the basis of what information? What would we want to change?

Having taken this time to identify things you might want to alter, I suggest adapting to implement the new learnings – yes, mid-exercise, that's fine – run a second scenario, and then see how using those updated processes and decision-making criteria make a difference. Or not.

This path generates a much more robust continuity plan that has been developed by all, not just a single subject matter expert. It therefore is 'owned' more widely and better understood.

### 5. Have a light footprint

As was identified by the SPR team in the post-mortem analysis, over-reliance on key infrastructure can be extremely debilitating. If all your IT systems and files sit within a single physical server, then you are very vulnerable. It isn't always practical or affordable to have backup servers or alternative HQ locations, so what else can we do?

Cloud-based systems are definitely an option to consider here, even though some question their security. A discussion should be had around the risks of cyber vulnerabilities versus the agility that cloud-based storage provides. The SPR team identified transfer of data from existing tapes after the fire as being something which slowed things down considerably. Imagine if all that data was available immediately.

Having a light footprint doesn't just apply to the digital sphere. There will be cultures and working methods which have 'always' been in place. Some of these are there for a reason – because they work – and should be protected, but not all.  Be sure to review how you do business on a frequent basis with a questioning eye to root out those processes which no longer make sense.

### 6. People are key

As is so often the case, our people are the best asset in any business contingency. This was a significant factor in how quickly SPR got itself back on its feet – with teams willing to come in and work around the clock due to their affection and loyalty to the company.

The lesson here is: care for your teams on a day-to-day basis, nurturing their personal and professional growth. This is morally the right thing to do, but it also protects the business. Look after your people and the people will look after the business.

This also applies to management following an incident. Do not underestimate the impact that a crisis can have on your teams, particularly if it involves loss of personal items due to a fire or flood. Make sure there are frameworks in place to catch employees who need support and you have a culture of talking to one another openly.

### IN SUMMARY…

Many of the above principles overlap. You keep agile by having a light footprint and not relying on key individuals. You challenge the status quo and gain early warning radars by consulting a 'vertical slice' of your people – not just the most senior leaders. What I mean by this is: don't see these principles as a checklist, more as an integrated framework. The case study on the next page, *Expect the unexpected – and plan for it*, is a good example. Connect all the dots and you will be in a much stronger position.