

In getting to grips with the unprecedented measures taken by governments around the world as they attempt to control the COVID-19 virus, it is safe to say that the last few weeks will have been an operational challenge for most organisations.

The tension between mitigating health risk and keeping the country 'open for business' has led to heated debate around Boris Johnson's models and policies, and on the rights and wrongs of his government's decisions – decisions which have triggered a significant economic shock, the full extent of which is unknown.

The pressure is already bearing down on businesses across a wide range of industries and sectors. The decline in second-quarter GDP is expected to be considerable, with travel, retail and hospitality bearing much of the brunt. The capacity of organisations to manage the operational and people risks is hugely varied; some are simply more prepared than others.

Business continuity industry veteran, Mike Osborne, says that while the sheer scale of the impact is unprecedented, the UK's history of emergency preparedness in responding to threats and incidents over the last 50 years makes the country far more experienced and better prepared than many others – particularly with the now added availability of high-speed networks and cloud computing. At the same time, he believes this experience could change businesses forever. "One thing my business continuity experience has taught me is that firms very rarely go back to being exactly as they were – this experience will fundamentally change business IT, working practices and processes," he opines.

Amongst those businesses, some will have invoked tried and tested

From chaos to continuity

The severity of the ongoing lockdown is forcing businesses to operate in ways that might transcend even the most frequently war-gamed scenarios. Deborah Ritchie reports

crisis management and contingency plans, others will have dusted off a plan that's not had the necessary attention or buy-in for however many months, and the rest will have just hit a very steep learning curve.

Regardless of where on that scale a business finds itself, the following perspectives may offer a refreshing view on how best to navigate this unprecedented time.

An IT continuity practitioner's perspective

From an IT perspective, correct purchasing and contracting of infrastructure should not be underestimated. The ability to flex services as and when you need to, rather than being tied into stringent contracts for the cost benefit, could make or break a business in the context of COVID-19.

If you have gone to the trouble of purchasing IT services to provide resilience, it's important they actually do that. Some companies may think they have that box ticked, only to find out too late that what they have bought does not actually meet their needs.

Take the example of a City firm which recently purchased adequate VPN licenses for everyone in the company, overlooking the fact that just a fifth of them could be used for remote working as part of the licensing agreement. To their credit,

this was discovered during testing, so the model could be fixed ahead of the event.

Having the correct number of concurrent remote connections is one thing, but if the networks the VPNs are trying to connect to don't have capacity in the bandwidth, the user experience will be severely degraded. It's not until you actually have live demand on your bandwidth that you can accurately assess whether your infrastructure is truly resilient.

Success when you most need it depends on a few key things. Most of them are clichés in our world but really do deliver your recovery for you.

Familiarity People knowing how to work from home without needing any support to do so – already having the kit, knowing how to use it, working remotely on a regular basis and being comfortable doing so.

Trained people Those engineers who look after our systems need the ability to be able to identify and rectify problems quickly, and be able to failover manually if automatic failover is unsuccessful. They also need to be able to do all of this remotely.

Trusted suppliers This comes back to the earlier point about purchasing. Lots of companies try to drive as much value as possible from their suppliers, however relationship management pays dividends when there are many companies vying for

attention – such as at times like this.

Resilience by design If you want to be resilient, you do need to invest. There is no getting away from this. Having good infrastructure architecture is the basis for good IT provision.

No matter how well prepared you are as a business, there will always be people who are reluctant or technically challenged to work remotely. Allowing for a reduction in productivity when planning for longer-term remote working is not a bad idea. Some people will be more productive at home, but this will be negated by those who are not as disciplined (probably because they don't often work remotely).

Finally, it is worth managing users' expectations about what their experience will be like when they're connected to corporate systems at home. People expect that the speed and service of, say, video conferencing will be exactly the same at home, not realising when they're in the office they're on an enterprise-grade network with significant bandwidth. Trying to video conference with Asia on a 17mbps copper wire broadband is not going to work as well.

The business continuity consultant's perspective

Les Price, head of availability services, Daisy Corporate Services

The scale, speed and severity of the COVID-19 threat is far greater than that of previous pandemics we've experienced, and response measures across the board have been scaled up accordingly. The UK has not seen this level of event since World War II. We have panic buying, infrastructure closing, lockdowns... the level of risk is unparalleled and the knock-on effects are where the biggest risks will ultimately emanate.

Since the last pandemic, we have

experienced a change in the use of our dedicated work area recovery services, with many customers using their suites frequently and for various reasons, not just for emergencies. This has contributed to a better, more organised response from customers who are now using our services to split critical teams.

Even the most well-prepared organisations are on the brink of the great unknown – it is unlikely many organisations have tested their remote working capability to the extent of having all staff working from home for an extended period of time.

IT departments will need to ensure all devices are monitored to keep users and the company infrastructure safe, as well as working to ensure the technology is delivering the expected levels of productivity for the business. It's inevitable that cyber criminals will take advantage during the outbreak, and we predicted that huge increase in the number of attack vectors caused by home working, disrupted processes, quickly introduced IT systems and so on. Security, therefore, is going to be a major focus throughout the pandemic.

Just how resilient companies are in the UK when it comes to IT continuity challenges of this magnitude, we will soon find out. From our experience, it's likely to be a mix of success stories, epic failures and muddling-through. I see this hinging on four core factors. Firstly, the maturity of the organisation's business continuity management planning. Secondly, the organisation's stage on their digital transformation journey. At this point in time, to illustrate these factors, we have our availability services teams busy working with our contracted business continuity customers while the rest of the business works to deliver

technology and solutions to those businesses who are less-prepared. Thirdly, the element of time. Unlike most disruptions where a percentage of business-critical staff can sustain operations for a given time, there is a concern that we are potentially facing months of disruption, and an organisation's resilience will depend on how well they will be able to manage and embrace change and adapt. This will literally be something that only time will tell, but experience of long-term invocations has shown us that the more time passes, the harder it is to keep control of the business and sustain values, culture and ultimately, revenues.

Lastly, the most important factor is people; this is also the most intricate, sensitive and unknown element. We are all dealing with the threat of COVID-19 on an individual level; no two people and their environments and experiences will be the same. Multiply this uncertainty by the number of staff you have to get an idea of the impact.

The insurance law perspective

Heidi Lawson, partner and Paul Moura, associate attorney at Cooley LLP

With the coronavirus, COVID-19, already taking its toll on the economy, are there any existing sources of insurance coverage to help cover the inevitable financial loss? With major sporting events, conferences, cruises and other excursions being cancelled as a result of the outbreak, including the cancellation of the 2020 Olympics in Tokyo, can a company look to its existing insurance portfolio and find any insurance coverage to help minimise the financial impact?

Traditionally, the most direct way to get insurance coverage for a disease outbreak is to obtain event cancellation coverage for events

cancelled or adversely impacted as a result of a disease or quarantine. To the extent a company purchases event cancellation insurance, events cancelled due to disease or quarantine may be expressly covered (or, in the case of very broad all-risk event cancellation coverage, not excluded).

However, without event cancellation coverage, most companies will need to hunt around for other possible sources of insurance. Political risk insurance, which many companies may already have due to international investments or overseas operations, may cover losses as a result of a government shutdown or curfews.

Unfortunately, with many political risk policies, this form of indemnity often necessitates a waiting period of 90 days or more prior to coverage activation. By the time the political risk policy takes force, there may be no need for it anymore.

Similarly, civil authority clauses in first-party policies can afford coverage for business income losses that arise when a civil authority prevents the policyholder from accessing their premises, which may happen when a civil authority blocks access to a property facing an outbreak. These coverages also typically have waiting periods (eg. 72 hours) before coverage can be triggered. Notably, such coverages will often depend on whether there is a requirement of physical loss, which may not be present in the case of an outbreak.

Directors and officers insurance coverage may apply if investors or customers eventually sue a company and its directors and officers as a result of losses incurred from breaching a quarantine or failing to take timely or appropriate action to mitigate the impact of a disease, resulting in additional sickness, a company shutdown and, eventually,

lost revenues as a result. However, one important thing to note is that many D&O policies have a broad bodily injury exclusion. As a result, coverage under a D&O policy depends on the precise policy wording and underlying facts.

Finally, another potential source of insurance might be under a company's employment practice liability insurance. EPLI can sometimes assist companies involved in actions by employees because of layoff or furlough claims due to government or company shutdowns.

To the extent that existing policies currently provide coverage, either directly or indirectly, we can expect that the insurance market will react quickly and add additional exclusions for disease or quarantines to many existing insurance policies, at least until the current outbreak subsides.

Pandemic planning

Roger Kember is former Deputy Director of Capabilities in the Civil Contingencies Secretariat, since the very first week of its existence. He instigated the Department of Health Pandemic Plan in (2001) and also wrote the national police pandemic plan. For 17 years, Roger also managed the police room in COBR. He is now a crisis management consultant.

When the Department of Health published its first UK Influenza Pandemic Preparedness Plan in 2001, the risk was based only on the flu virus, with the 50 million plus deaths worldwide from the Spanish Flu Pandemic of 1918-19 the worst-case benchmark. Seasonal flu will always be with us as well as spikes from new strains of the flu virus, as in 2008-09. We are still waiting for the 'big one' (expected to be a variant of avian flu), so, the 2001 Plan (including its slight revisions over the years) will still hold good.

Scientifically, the coronavirus is different from the influenza virus, but these two viruses have as many differences within themselves as between themselves. We've had mild flu outbreaks as well as severe ones. The coronaviruses SARS and MERS had high mortality rates but did not spread worldwide as the variant responsible for COVID-19 has.

These differences are important to doctors but to business continuity professionals, businesses and other organisations, the impact of a pandemic (whatever the virus) is the same: human beings are quarantined, ill, recovering, caring for family or succumb to the infection.

Taking so many people out of circulation at the same time and all around our interconnected world has a significant business impact on production, logistics, services and markets. It also has social, personal and family impacts both practically and psychologically. Many businesses say that 'our people are our most important resource': a pandemic tests this statement to the limit.

This outbreak is characterised by the definition of a 'crisis': "An abnormal and unstable situation that threatens the organisation's strategic objectives, reputation or viability." (Crisis Management: Guidance & Good Practice BS 11200).

Medically, it's a new virus; there's no vaccine; its lifecycle is only partially known; viral shedding (infectiousness) can last for 24 days (ie. 10 more than the government advised quarantine period) and we don't know if it will mutate (like 'flu) and hit us with a new variant every year.

Business-wise, the world is a very different place today compared with 2001, so the learning from past flu pandemics is only a partial help.

Businesses have suffered the triple

blow of a supply crunch, a demand slump and a cash-flow constriction.

This has been the first pandemic to hit the world after China has earned itself the moniker of 'workshop of the world'. Globalisation of supplies and cheaper costs there have made the world dependant on it for a range of goods, from electronic components used in ventilators to hand sanitisers. China is the largest manufacturer of generic drugs and produces 80 per cent of the world's basic active pharmaceutical ingredients. India is the world's second largest producer of generic drugs but imports 75 per cent of its APIs from China.

Demand for everyday groceries has spiked due to stockpiling but demand has slumped to near-zero in the tourism leisure and hospitality sectors and associated industries of airlines, credit card companies, breweries and professional catering supplies. So long as self-isolation continues, so too will the demand slump.

No sales equals no income. Every bankruptcy leaves bad debts. Staff layoffs result in reduced demand from consumers, which means reduced sales and reduced cashflow. This is where the world economy was in the Great Depression. Fortunately, present governments are following Keynesian economics and have declared they will pump government money into the economy and suspend some tax burdens from businesses for the time being. There is not yet complete clarity on how some of these will be put into effect and it is still too early to determine if these provisions will be sufficient.

There are a number of 'firsts' associated with this pandemic.

China as the workshop of the world and the knock-on problems of supplies and the logistical movement of shipping containers. (China has made a number of strategic decisions

on trade including its programme to become the world's dominant maritime nation and maritime insurer). Indigenous industries in the west have largely gone to the wall unable to beat China's pricing policies. For many products, we have no UK suppliers. We have a chronic shortage of personal protection equipment for the health service, care workers and others on the COVID-19 front line.

It's the first to hit the UK after its 'Cold War Dividend' changed the government's strategic thinking. Until the fall of the Soviet Union, the UK (and ATO countries) protected its strategic industries: principally the defence sector, but also the security of government communications networks. With the end of the Cold War, the government decided there was no longer any threat to the UK and drastically reduced its subsidies and funding to these defence-critical industries.

We are now in the age of social media. It is being used by the government to get its infection control measures out to the public and official guidance is available everywhere online. Social media is also being used to overcome the loneliness of self-isolation. Local community support groups are using Facebook and other apps to keep in touch with those who may need help and support. The flip side is the scammers and conspiracy theorists are already at work. A crunch point will come if the number of patients needing ventilator support vastly exceeds the ventilators available and people die who otherwise might have been saved. The burden will fall on doctors to decide who lives, and that will be impossible to keep off social media.

Working from home has become a fact of business life. It may even become a mainstream feature in the same way that open-plan offices and hot-desking has been factored

into cost reduction. With schools, colleges and universities closed, it will be a full-load test of the domestic broadband capacity with users streaming, playing interactive games, Skyping/Zooming and downloading while others are trying to connect to work servers.

The fifth element is the government's issue of emergency powers, how these will be enforced and what the public reaction to them might be. In crisis management, it is always wise to undertake some 'worst case scenario' planning. My potential worst cases are:

- This coronavirus will return in waves (the Spanish Flu had three waves)
- It mutates, like the flu virus, and will threaten the world with a new outbreak (of unpredictable severity) every winter
- We get a flu pandemic and coronavirus pandemic at the same time
- We suffer a different crisis at the same time (eg. solar flare, flooding, oil shortage, extensive cyber attacks or major military confrontation).

Everyone is doing their best to deal with this situation using their existing pandemic plan and there is a lot to do on a day-to-day basis. Everyone will need a coronavirus pandemic plan as well as their flu plan. Make the time now to take stock of your pandemic response and coronavirus business continuity plan and revise them in the light of your experience to get effective day-to-day management (ie. 'command and control') and give top management the head room to consider the strategic issues for now and the post COVID-19 world.

▶ Deborah Ritchie is group editor of CIR Magazine