

The business impact may be felt in a variety of ways:

- People will be seeking information – communication systems may fail;
- Key personnel may be unavailable for lengthy periods (permanently in a worst case scenario) – apart from those falling to the disease, many people may choose to stay at home rather than risk exposure;
- Offices may be voluntarily closed;
- Offices may be closed by health authorities;
- Transport systems may be disrupted;
- Movement of people may be restricted;
- Suppliers may be forced to close;
- Customer base may decline as client organisations are forced to close, or people avoid populated environments such as shopping centres
- Panic-based evacuations may be attempted;
- Law and order may suffer;
- Litigation may result from claims centred around air conditioning, duty of care, etc;
- Authorities may not be able to cope if numbers of sick and dying exceed expectations (who would have believed the chaos of New Orleans ?).

One of the greatest risks is panic and its possible outcomes. People will adopt a siege mentality wanting to stay in their own homes, surround themselves with their loved ones, and avoid any non-essential interaction with other people. A job pales into insignificance when life and family are under threat.

What can organisations do in terms of business continuity management? A key platform of business continuity is providing business resilience – reducing the likelihood of an interruption occurring and reducing its impact if and when an incident does occur. If we examine some of the possible impacts listed above effective planning might include such measures as:

- Implementing effective knowledge management – this includes:
 - Completion of a critical records analysis;
 - Provision of Standard Operating Procedures;
 - Cross-skilling for key employees;
 - Ensuring that knowledge and skills is distributed across interstate or geographically dispersed branch offices;
 - Succession planning;
 - Capture and management of critical information;
 - Off-site storage of copies of all critical information.
- Communications issues must be a priority:
 - Ensure that all contact lists are up to date and maintained;
 - Evaluate all communication options to keep personnel informed – mobile network, PSTN, 1800 number (in Australia) , radio, internet, intranet, etc;
 - Establish means to communicate with suppliers;
 - Establish means to communicate with your customer base;
 - Establish an authorised and competent team to communicate with key stakeholders and the media;
 - Consider remotely hosted email and website options;
 - Consider alternate telephone providers if this gives you redundant systems.
- Planning for flexible work practices including:
 - Working from interstate/branch offices;
 - Working from home;
 - Moving personnel to other locations (may need to accommodate families);
 - Leasing remote facilities (safe areas) and relocating personnel;

- Developing key resourcing requirements for each of the options;
- Your business continuity plans will need to cater for all of these options including provision of ICT facilities, etc.

- Provide secure transport:
 - Contract with a bus company to provide private transport for employees;
 - Establish a car pool system.

- Review your supply chain:
 - Contract multiple suppliers;
 - Look for geographic dispersion (even international);
 - Know who are other key customers and where you stand in the “pecking order”;
 - Ensure that your suppliers have effective and thoroughly tested business continuity plans.

- Review your customer base and other income producing opportunities:
 - Can you expand upon your existing customer base;
 - Are there distribution and delivery options that reduce the need for movement of people;
 - What about global markets;
 - Can you diversify your product set and expand your customer base;
 - What hedging opportunities may be available to spread your risk.

- Law and order – security:
 - Do you have arrangements in place to secure your premises for short and long term periods of vacancy;
 - Know who else uses the services of your security provider and what priority you will receive if the security provider receives multiple demands for increased resources;
 - Consider plans for security of personnel at all times – in the office, travelling between home and office, security at home;
 - Consider planning for secure provision of consumer staples – food, drink, essential household items. This could involve bulk purchasing arrangements, escorted shopping groups, etc;
 - Have a named contact within the police and emergency services organisations and provide them with a named contact and alternate within your organisation. Your contact must be able to make decisions;
 - Meet with and understand the plans and limitations of local police and emergency services.

- Legal, regulatory and insurance
 - Carefully examine all aspects of your insurance policies – are you covered for all cases of business cessation including voluntary closure, mandatory closure (emergency services), etc;
 - Are you adequately covered for loss of income;
 - If an employee contracts the disease will you have any liability, are you insured;
 - Ensure that you regularly inspect air conditioning plant and all shared washroom facilities to guarantee health standards.

It is worth noting that many of the issues potentially arising from a pandemic would also apply to a Chemical, Biological, Radiological or Nuclear (CBRN) incident and to a major flood incident. A pandemic and a flood would both include warning periods although, as we have recently seen in the USA that does not always guarantee an effective response. In the case of a CBRN incident there would be no warning.

A key issue, here, is the critical need to keep exercising your plans – until you have exercised your plans you have no idea if they will work, or simply worsen the situation. Exercising also develops a business continuity management culture and a level of skill in the participants that will be essential in the management of a real incident. There are two quotations that precisely sum up this requirement and which make a fitting conclusion to this article:

“Plans are nothing, planning is everything” - Dwight D Eisenhower

“No plan ever survives contact with the enemy” - Helmuth von Moltke

Identify your mission critical activities, consider the risks, develop your plans, but then exercise, exercise, exercise.

How organisations should prepare for bird flu

Include the possibility of an avian flu pandemic in your business continuity planning and crisis management preparations. Gartner points out that a pandemic wouldn't affect IT systems directly, but it would likely cause considerable economic disruption through its impact on the workforce and on business activity.

IT managers can plan for threats such as avian flu because many contingency strategies use IT to keep business running – even with travel restrictions, quarantines or problems with vendors or employees because of illness or fear. IT managers should ensure that their organisations plan for a possible outbreak whose course and consequences are unpredictable.

Use scenario planning to assess possible business impact and as the basis for developing appropriate contingency plans for different situations, says Gartner.

The 2003 SARS outbreak suggests that a pandemic may have the following effects:

- International travel: Depending on the severity of the outbreak, quarantines may result in travel bans or travel delays. Health checks for travellers would likely be commonplace. Many trips could be cancelled.
- Local travel: In cities or countries where an outbreak occurs, travel may be severely restricted or even impossible for periods of time.
- School closures: Schools in affected cities would likely close, forcing many parents to stay home and care for their families.
- Health systems: Medical facilities could be overwhelmed, depending on the size and virulence of the outbreak – particularly in less-developed nations with already-strained healthcare resources. As with SARS, containment methods would likely be low-tech, relying on awareness campaigns, surgical masks and isolation.
- Economic impact: Experience with SARS demonstrated that industry sectors such as travel and hospitality would be rapidly affected, with flow-on effects occurring in other parts of the economy. Some sectors, however, would benefit, such as technology companies that provide solutions for remote workplaces – but this would be small compared with normal business operations. The effect on individual communities could be prolonged if outbreaks recur, as has happened during previous flu pandemics.
- Supply chains would likely be affected because of inspections and logistics disruptions, especially where countries with high infection rates are involved. Also, certain animal products or other products might be banned.
- Personnel: Widespread illness could result in staff shortages for providing essential community services – particularly in medical staffs.
- Overall business slowdown: With travel limited and spending reduced in many areas, sales and marketing campaigns would be affected. Deals and transactions – domestic and offshore – could be delayed.
- Fear, uncertainty and doubt (FUD): Even if only a few people are infected, the threat of disease could greatly affect the behaviour and normal business activities

of others. Discussion and speculation about the situation would further reduce workforce productivity.

Don't wait for an outbreak to review or establish contingency plans, urge the researchers. Many strategies take time to set up. Gartner recommends the following key activities:

- Make your workforce aware of the avian flu threat and the steps you're taking to prepare for it.
- Assess your business continuity preparedness for this type of workforce outage scenario and try to improve it (if necessary).
- Assign someone in your business to track biological threats such as the avian flu. He or she should regularly review business continuity plans and update them in response to new information.
- Establish or expand policies and tools that enable employees to work from home with broadband access, appropriate security and network access to applications.
- Expand online transaction and self-service options for customers and partners.
- Work with customers and partners to minimise any disruption by developing coordinated crisis response capabilities.