

# Risk mitigation measures

Without mitigation measures and tried and tested plans in place organisations can lose revenue, reputation, not to mention customers or the entire business

Managing meltdown and mitigation measures are mandatory and a core competence in UK business, with 2007 witnessing BC and risk reputation increasing (though not fast enough) in the demanding domain of the Boardroom.

There is at last an increasing awareness among BC professionals of the reputation aspects of their work in both anticipating the kind of incidents that can affect an organisation and planning for them to ensure the business can function in a threatening and emergency situation.

BC vendors have a vibrancy in the market place which must be recognised by all stakeholders – at the end of the day it is their work that will make an organisation survive catastrophe and protect their staff, supply chains, information availability and assets when faced with disruptive threats.

With this in mind that it is all credit to the leading Business Availability Group ICM that it collected two awards at the CIR Business Continuity Awards.

Mike Osborne, ICM's Managing Director of Business Continuity, says "With supply chain continuity a key concern within the marketplace, the development of the BS25999 industry standard for business continuity demonstrates that it is in the interests of the UK economy to ensure that all organisations receive education, assistance and affordable service in their business continuity provision, irrespective of size."

It may be impossible to plan for every eventuality and vulnerability to disaster scenarios, but enterprises can still take steps to protect themselves from most risks when suppliers themselves are ensuring business



continuity is accessible to all companies to allow them to build BC solutions to ensure a continuity supply no matter what.

Deputy Chief Constable (DCC) Andy Trotter, British Transport Police, presented to industry leaders and continuity professionals the resilience required to deal

with terrorism threats. He also covered other BC aspects for organisations' protection and continuity interruptions. Reviewing the evolving threats – both internal and external – facing large organisations through to SMEs.

The DCC pointed out the business communities' vulnerabilities when faced with internal and international threats. Trotter explained that many UK Boardrooms are not expert at ensuring a business continuity management (BCM) culture, which is essential following critical incident.

People are the most challenging aspect of BCM and he urged executives to take a long, hard look at how they safeguard their workplace, supply chains, information data – the effective maintenance and monitoring measures of their essential services and critical functions when protecting their business.

"In the absence of widespread buy-in, a significant proportion of a BC manager's effort will be wasted, leading to frustration and under-achievement, whilst leaving the organisation exposed and vulnerable, said Trotter."

Strategies for measuring the firm's "continuity culture" are key as well as new thought processes and attitudes toward risk and effective communication. As no two cultures are the same BC managers are faced with reconciling regulatory rigorous intent

with their own company's personality. This is a tough challenge, requiring insight, imagination, innovation and insatiability.

Graphic (1) shows a number, but not all, of the vulnerabilities and particularly highlights the supply chain issues which must always be considered in any strategy to protect business, environment and mitigate measures.

"Plans were on the shelf and had not been revised to cope. The defects were there and the basics were not."

There are a number of issues which show inextricable links between some common business practices and other areas, sometimes not considered in business terms e.g. poor information sharing between rivals. There are times when commercial sensitivities may have to come second place to the risk from threats and some common sharing of information could benefit all concerned.

Bruce Mann, Head of the Civil Contingencies Secretariat has much on his desk when

considering UK businesses planning assumptions – loss of staff, facilities and access denied to main premises and information for many months from incidents ranging through terrorism, loss of mains electricity or water supply for up to three days locally or a significant disruption to fuel supply and transport for up to 10 days.

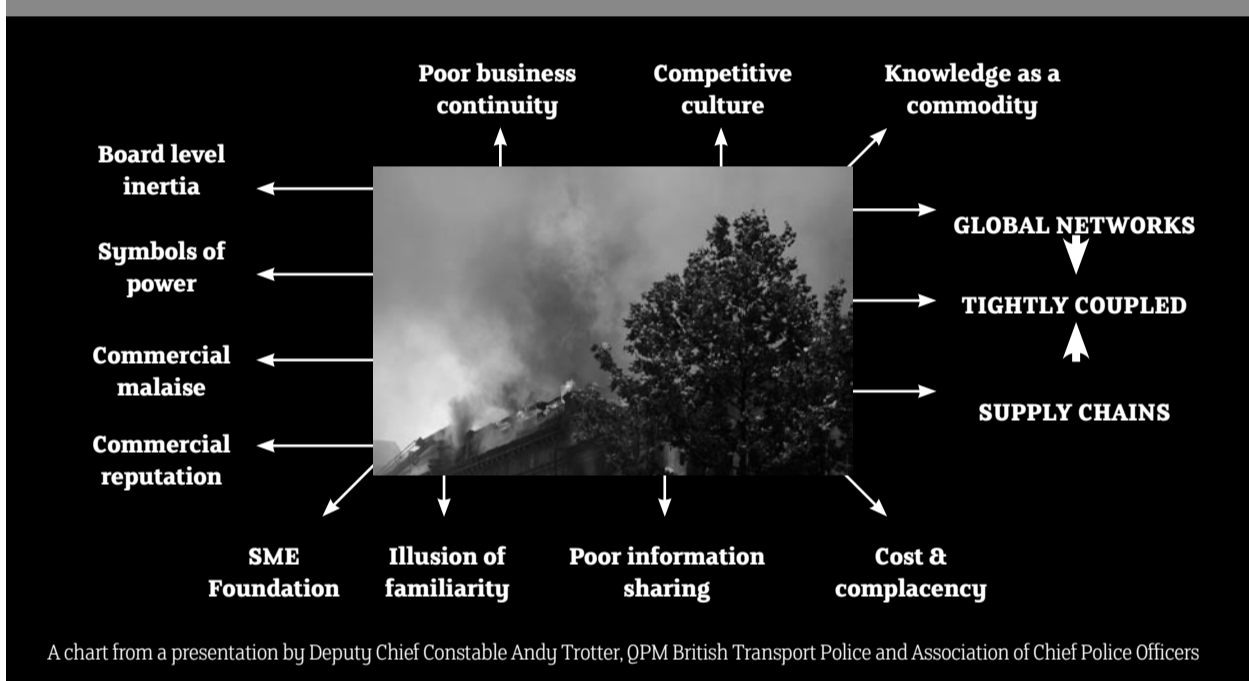
"Whilst we have learned from millennium emergencies, incidents have exposed serious deficiencies. Plans were on the shelf and had not been revised to cope. The defects were there and the basics were not."

Never was there a more appropriate time to heed Mann's words for 2007. ▶

## Did you know? ?

- 80% of businesses, without a BC plan, close within 18 months of a major incident
- 90% of businesses who lose data from a disaster are forced to shut within two years
- The Home Office estimates that nearly one in five businesses suffer a major disruption on average every 5 years

### GRAPHIC 1: PRIVATE SECTOR VULNERABILITIES AND INTERNATIONAL TERRORISM



# Pandemic Influenza - the threat to business

CEO of UK Occupational Health Provider Healthcare Connections Ltd speaks out

Experts at the World Health Organisation (WHO) and elsewhere believe that the world is now closer to another influenza pandemic than at any time since 1968, when the last of the previous century's three pandemics occurred. A global pandemic could infect 1 billion people and kill between 2 and 7 million.

A pandemic in the UK could overwhelm the country's health and medical capabilities potentially resulting in millions of hospitalisations, and hundreds of billions of pounds in direct and indirect costs. By the end of the pandemic up to half of the UK population could have developed influenza and between 50,000 and 750,000 deaths could occur. This would in turn impact heavily on business which could face an absenteeism rate of 50%.



Healthcare Connections first encountered the worrying subject of pandemic influenza in 2003 and immediately wanted to take action. HCC (Healthcare Connections Ltd) began working to provide the right protection to our own employees and this quickly grew into our bespoke occupational health offering for business.

In the beginning, HCC became aware of the limitations that businesses faced. Offering



employees a vaccine would not be possible because a 'strain-specific' vaccination (for an emerging pandemic) cannot be manufactured until the strain is identified, and this cannot happen until the virus emerges. It would take up to six months to manufacture, distribute and administer the vaccination, by which time it would be too late for many people.

Therefore the natural progression for HCC was the use of antiviral medication to reduce the severity and duration of illness. The advantage of antiviral medication is it can be used to work on the differing strains of influenza, as well as being able to be widely prescribed and easy to administer (capsules). This is what we offer our clients

under a full occupational health scheme to safeguard employees against a pandemic and the resulting business implications.

We felt very strongly that this medication should be a service offering for corporate clients and, as a result, HCC have been in talks with the manufacturer of the medication since 2004. This allowed HCC to begin implementing client schemes quickly and ensures that we can continue to secure medication orders efficiently. The Department of Health, WHO and other health organisations are taking this threat very seriously and so should UK businesses. The HCC service is unique in that, not only do we offer cover to our corporate clients, but also to other members of their household.

The UK government has stockpiled over 14 million doses of antiviral medication, with priority for treatment given to frontline workers, essential service providers and people that fall into an 'at risk' health group. With a possible 50% of the population susceptible to catching influenza, HCC advises businesses that they should act to protect themselves, as it is only a matter of when, not if the pandemic hits the UK. ▶

**Alison Brown, CEO National Healthcare Connections Ltd.**

**See the HCC advertisement on page 2. For more information please call 08456 773005 or click on www.hccpandemic.com**

## VoIP security

Internet telephony can cut costs – but good safety systems are essential

Companies' data networks have long used a communications protocol (i.e. rules for formatting and transmitting the information) called Internet Protocol, or IP. By contrast, voice traffic has used different protocols.

However, moves are afoot to put voice communications onto IP networks. The promise of voice over IP (VoIP) is that voice and data can run over the same network, meaning lower cost.

There are also risks, though. When voice runs over the same network as data, if the network goes down, you are incommunicado, unless you can revert to the traditional telephone network.

Graham Chick, CEO of UK telecom solutions developer Gematech says "before embarking on an expensive upgrade to embrace VoIP think carefully about how you are going to support and maintain your new technology when you turn up for work one morning to find your combined voice and data network isn't working."

While acknowledging that it holds enormous promise, Gematech's Chick

says VoIP has been depicted as a universal panacea by some overzealous salespeople, but that in reality it requires a lot of reflection before taking the plunge.

"Because VoIP makes use of so many sub-systems and other standards, even more than a typical PC network, a simple issue, like a well intentioned employee plugging in a home WiFi router for a guest so they can use their laptop could cause a sequence of events that are not initially obvious, but none the less causing catastrophic failure of an entire network over hours days or weeks," he comments.

Equally, troubleshooting is a very different activity in the world of VoIP. "A conventional phone system failure is simple to resolve: it will be connectivity to site, the PABX, or a power issue, all easily identified and planned for. In contrast a failure of a VoIP system could be due to a fault or miss configuration of one or more of a number of systems. Most IT departments don't have the equipment or skills to fault-find or resolve a major problem in a realistic period of time." ▶