

Will your business survive a terrorist attack?

White Paper



InTechnology
for Business Continuity Computing

A practical approach to assuring business continuity

Summary

The new dimension in terrorist threats targeted at civilian businesses means that whole city centres may be damaged and inaccessible for years to come. A fundamental shift in business continuity thinking is required.

Traditionally, businesses have stored their critical business data and systems under lock and key in a vault on their own premises or a nearby city repository.

With the new level of threat, business data and applications will only be secure if copies are held remotely, far away from the dangerous city centre zone. The new generation of high-speed, low-cost communications makes the siting of critical data in a remote data centre or "bunker" a rational and robust strategy that will ensure businesses can survive a disaster.

In case of attack, normal business operations can be rapidly resumed with staff working from home or other temporary offices, accessing data and applications remotely. If the business escapes attack, there are other powerful benefits in a cost-effective and secure data storage solution.

Background

Terrorism and the threat of terrorism are part of today's society and, unfortunately, are here to stay. The threat affects all parts of the UK and the Government takes the threat seriously enough to deploy troops in and around key locations to provide assistance to the police.

The move to an "information global village", with businesses reliant on their IT applications and data, means that they are vulnerable to attack in the city centre locations where their IT systems are held. Along with the rest of the civilian population, business in Britain is therefore experiencing a significant growth in the level of threat that has not been seen since the end of the Second World War. While the attacks of September 11th proved that major attacks could be launched with devastating effect at city centres, bomb outrages in UK, such as the attack on Manchester City Centre, have similarly shocked and damaged the city; bombings, such as the Harrods bombing and Bishopgate brought casualties and major disruption to London.

Now a general threat of attack has now been made to many cities outside of the capital, and the Government is actively making preparations to deal with the after-effects, including possible radioactive 'dirty bombs', which may minimise the number of casualties but make whole areas uninhabitable for up to 20 years. It is estimated there are approximately 4000 businesses outside London sited within 5km of some 20 vulnerable city centres.

Businesses are quite rightly focusing their primary efforts on providing maximum security for their staff in case of an attack and it is of paramount importance that this contingency planning should be driven from board level.

Company directors also have a duty to protect the business itself, for the sake of their staff, shareholders and customers, taking practical steps to ensure that the business can survive an attack and continue to provide a service as soon as possible afterwards.

Evidence from the Manchester bombing makes grim reading for business managers. Figures on the Home Office website, (www.homeoffice.gov.uk) show that:

- over 670 businesses were affected
- £5m of business was lost within the first few hours
- communications were not fully restored for 48 hours
- certain areas were not accessible for up to 5 days.

These figures themselves paint a picture of catastrophe for Manchester business, but consider this was 7 years ago – how much more dependency is there on IT now? The question posed by the Home Office report is clear: **"If your company had been affected, would you be in business today?"**

The increasing dependence on IT systems and data means that the potential damage today would be greater. Warnings of estimated consequences from the finance sector are stark.

Speaking on a recent Channel 4 news item about the potential cost of an incident today, Michael Foot, Managing Director of the Financial Services Authority, said: **"Essentially, that day, billions and billions – probably trillions – of dollars, pounds and euros wouldn't flow to their correct home. As the day went on, you could get an enormous economic jolt through to real trade, investment markets. Stock markets and so on would be very badly affected when they came back on again. Liquidity they thought they had wouldn't be there. Over time, what you would get would be international firms looking at New York, Tokyo, London; they would assess which one had failed to deliver. And they would cut back investment there, leading to cuts in employment, and they would take to business to places which have proved resilient."**

Building a Business Continuity Plan

Any manager addressing business continuity issues in the current climate needs to focus on safeguarding, first, people, and secondly IT applications and data.

Businesses today depend for their viability and daily operations on IT systems and the critical data in those systems – client lists, price lists, details of current transactions, purchase ledgers and sales ledgers.

Many businesses store and backup this critical data on tape, and hold copies in safes on or near their premises, changing the tapes manually each day and transferring them via courier to the safes. Disaster recovery plans have centred around renting of nearby office space, with secondary IT systems and desktop PCs provided. The main threats to business systems have been thought to be human error, fire or flood.

Whilst in general these DR plans have never been tested to destruction, the strategy has been adequate in the past. They are clearly inappropriate in a climate of risk where a major city centre attack threatens to make all the business buildings in the city inaccessible for many years.

Not only is there a risk of staff casualties, but the building will be inaccessible for a period of time. This could be a matter of days, in the case of recovery of criminal evidence, or years in the case of chemical or biological attack. Communications may not be in place, and the sheer logistical problem of emergency services coping with an incident will make entry to a normal place of work almost impossible.

Business Continuity Computing

Many companies have in the past used a strategy of a second site to hold either a point-in-time copy of their data or a complete mirror image of their critical systems. Using previous generations of technology, these **"remote"** sites tended to be within a short distance of the primary site. The reason for this was simply the speed and cost of the network required to link the sites together. It has been too expensive to meet the demands of both speed and distance.

Using the latest generation of optical fibre networks, the distances can be greatly extended without compromise on speed or cost. Now remote data centres can be truly remote, not only vast distances from the capital but also from any other city.

Remote data centres are now available to customers, both large and small, with the advances in network technology bringing the benefits of cost-effective delivery. By linking into the network, staff can ensure businesses continue to perform from almost anywhere in the world.

Managed Data Services as a way forward

New low-cost communications and data storage technologies mean that business managers have the means through Managed Data Services to protect their business from the level of attack which is currently threatened.

With Managed Data Services key applications and critical business data can be replicated on site and transferred via secure communications links to a data centre, where they are expertly managed and securely held 24 x 7. The data centre **"bunker"** is well away from city centres and outside of built up areas.

Switchable communications will then allow access from anywhere, maintaining a near to normal service. Staff, working from home or from alternative locations, can access applications and work on current data to keep the business going.

The key to setting up such a plan is timing. Instigating such a plan today is clearly a sensible business strategy. The companies who do invest today and have a plan as to how to minimize disruption will be the ones that survive.

"Since the 11 September terrorist attacks, we have worked to strengthen the FSA's contingency arrangements against an emergency event which would close our main office in Canary Wharf," said Financial Services Association Managing Director Michael Foot. **"We have developed a fully operational back-up site and run simulations of emergency events to prepare our staff and to test our infrastructure to deal with an event that would interrupt the normal operation of the financial services sector. Our guidance to firms is that they should have in place appropriate arrangements to help them maintain the continuity of their businesses in the event of an interruption."**

Today is not too late!

Assuring the integrity and security of IT systems and data as part of business continuity planning is not a large-scale or complex task. The technologies involved are robust and well-established. Managed Data Services can be set up in a matter of weeks.

InTechnology – specialists in business continuity

InTechnology has been supporting major public and private sector clients with data security strategies for 20 years and has invested in the data centre and communications infrastructure which are needed to provide secure Managed Data Services to businesses in today's climate of risk.

The first stage in installing Managed Data Services is to carefully assess what the core applications are. Using its own consultants, InTechnology can advise on the correct strategy to use to achieve the desired results.

This assessment is followed by a design service, installation, implementation and, most importantly, data management. Areas which can be covered include offsite data storage, the ability to recover in the shortest possible time, replication at all levels, hosting and above all management. InTechnology support personnel are on hand twenty four hours a day to provide assistance in recovering vital data.

InTechnology has multiple data centre bunkers which can be used not only for storing data but also for hosting complete systems.

Delivery to and from customer sites is via InTechnology's own network, LANnet which as its name suggests provides a virtual extension to the customer's own LAN. Running at up to 2.4Gb/second, fast recovery is guaranteed. Customers can also benefit from using it to save costs on Internet connectivity and/or Virtual Private Networks which can provide high speed linking of a company's sites.

Finally, to ensure the data does get backed up (or recovered), InTechnology provides the systems to achieve this with little or no requirement from the customer.

Now a Business Continuity Plan can be instigated, tested and ready for use in the shortest possible time using InTechnology Managed Services.

Next step

For more information on how to protect your business, call InTechnology on **01423.850000** or visit www.intechnology.co.uk