



CONTINUITY PLANNING

CONTINUITY PLANNING

Could your business recover and continue trading after a major security incident?

Accidents, criminal acts, vandalism, natural disasters, terrorist attacks and security breaches at some point in the future could affect the operation of your company. Do you have contingencies in place when such events occur? Could your business recover and continue to trade after a major security incident?

Every year nearly one in five businesses suffers a major disruption. Planning to deal with those disruptions is widely regarded as good business sense.

Outside forces can damage your business, be it an act of sabotage or a catastrophic explosion which not only affects you but the whole operation and infrastructure of your business.

A major terrorist incident could have the following consequences:

- Loss of staff through death or injury.
- Damage to your buildings.
- Loss of IT systems, records, communications and other facilities.
- Unavailability of staff because of disruption to transport or their unwillingness to travel.

- Adverse psychological effects on staff, including stress and demoralisation.
- Disruption to other organisations and businesses on which you may depend.
- Damage to reputation.
- Changes in the business demands placed on your company.

You will need the right resources to maintain your critical business functions. These are likely to include:

- Sufficient people with necessary expertise and motivation to lead and manage the organisation.
- Access to key records and IT systems.
- Reliable means of communication, especially with your staff.
- The ability to carry on paying staff, to ensure their safety and to provide them with welfare and accommodation.
- The ability to procure goods and services.
- The ability to respond to demands from the media.

THE IMPORTANCE OF PLANNING

External security incidents may be beyond your control but by having tried and tested plans in place, coupled with highly trained and capable personnel, your company will be able to cope and recover.



CONTINGENCY PLANNING, DISASTER RECOVERY AND BUSINESS CONTINUITY

There is often a lack of understanding as to what is a contingency, a business-continuity and a disaster-recovery plan. This often hampers the performance of your security people in a crisis situation.

PLAN	DEFINITION
Contingency	Are you able to reduce the probability of a security breach and are you able to prevent security risks from occurring
Disaster Recovery	Ensures that alternative back ups to core business assets such as networks, facilities, computer and IT are available in the event of a major security incident
Business Continuity	Plans and procedures to ensure that you can return to the minimum operating efficiency in the minimum amount of time from the occurrence of a major security incident.

You may find the definitions above useful when developing your plans

DEVELOPING AND MAINTAINING AN EFFECTIVE PLAN

Your plan should only include that which is relevant to sustaining the security of your business and your personnel. The plan should make sense to all staff and be communicated effectively across your business.

ADVANTAGES OF MULTI-SKILLED SECURITY OFFICERS

In the past, many companies had designated Security Officers, Fire Wardens, First Aiders and Health and Safety Officers. However, recent times have seen the emergence of the multi-skilled security officer trained to cover additional responsibilities such as:

THEN	NOW
Security Guards	Security Officers
Fire Wardens	Security Officers Fire Wardens
First Aid	Security officers and First Aid
Health and Safety officers	Security Officers and HSE
DISADVANTAGES	ADVANTAGES
Ring-fenced functions	Cross Compliance
Limited Flexibility	Better understanding of Security Technology
More Cost	24/7 Support for key functions Better Security officer integration with core business Cost Effective Better security officer continuity and retention Peace of mind

Having multi-skilled security personnel can offer you more protection and greater flexibility under continuity and disaster recovery plans.

NATIONAL CONTINGENCY SUPPORT PROGRAMMES

At the local level, the Civil Contingencies Act 2004 requires local authorities to provide advice and assistance to businesses in relation to business continuity management. You should consult your Local Authority website for further details.

There are also programmes across the UK that you may be able to tap into when developing your own contingency plans.

Case Study: City of London Police-Project Griffin

Developed by the City of London Police, Project Griffin has a remit to advise and familiarise managers, security officers and employees of large public and private sector organisations across the capital on security, counter-terrorism and crime prevention. The Project brings together and coordinates the resources of the police, emergency services, local authorities, business and the private sector security industry.

Organisations registered with the Project take part in a one day security-focused seminar, which can be geared to their specific needs. This enables organisations to target their specific concerns whilst sharing best practice across a range of security issues. This is followed up 12 months later by an online refresher package.

Following its success in London, Project Griffin has now been adopted by over 20 other UK police forces, and has generated interest and acclaim from overseas (Hong Kong, Australia and the US in particular)

www.projectgriffin.org.uk

Corporation of London

In 2004 the government introduced the Civil Contingencies Act to enhance the capabilities of the Corporation of London to respond efficiently to emergencies. It covers the way the Police and local authorities plan and prepare for security incidents.

This legislation requires the emergency services to communicate and work together on all aspects of emergency planning.

The Corporation of London and the City of London Police have established the City of London Contingency Planning Team (COLCPT) to help the city businesses to be more efficient in their response to security emergencies.

Project Argus

Project Argus is a National Counter Terrorism Security Office (NaCTSO) initiative which explores ways to help organisations prevent, handle and recover from a terrorist attack. It achieves this by taking businesses through a simulated terrorist attack. The event allows the client to explore their options; what is likely to happen in the event of a terrorist attack; how their continuity plans (if any) function, and what their priorities should be. The events are free and are ideal for businesses of any size. The events take place around the country and have involved constabularies from around the country, including Merseyside, Bedfordshire, North Wales and Cambridgeshire.

www.nactso.gov.uk

CONTINGENCY PLANNING SAVES LIVES

When those two planes struck the Twin Towers on September 11th 2001, Morgan Stanley activated their contingency and continuity plan to safeguard the lives of their employees. In the first 20 minutes between the first and second planes crashing, their evacuation plan was implemented.

This plan was developed after the 1993 terrorist attack on the World Trade Centre. Most of the 3,700 employees were off the high floors by the time the second plane struck. Six employees were killed in the attacks; considerably fewer than other businesses in the Twin Towers.

Operations managers acted promptly to ensure Morgan Stanley could continue operating. Employees walked 22 blocks to their back-up site to turn the computers on.

By 9:20am the back-up site was live and by 9:30am senior management had relocated to another back-up site that became their command facility.

25 years of expertise providing total security solutions



In the attempt to locate their 3,700 employees, as per the plan, Morgan Stanley converted one of their credit card facilities in Phoenix to a toll free emergency hotline. By 11 am the number was appearing on national television and by 1:30pm the centre had received over 2,500 calls. New York's City's phone system suffered failures within one hour of the attacks so Morgan Stanley accessed a dedicated phone line to their London office, which enabled them to call their Chicago Office.

Morgan Stanley recognised that it was not only important to get back to business quickly and as efficiently as possible but that it had to ensure that its employees were coping with the situation. Three hundred grief counsellors were hired to help traumatised employees and to train managers on how to respond to their fellow employee's difficulties in coping with the aftermath of the incident.

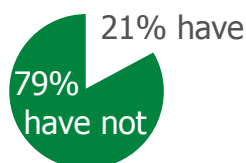
A key part of Morgan Stanley's efficient reaction during this incident was the way in which their highly trained security personnel responded.

ARE YOU PREPARED?

Businesses need to be prepared for any eventuality. In 2005 the explosion at the Buncefield Depot in Hemel Hempstead caused huge disruption in the South East; this and other events, such as 7/7 in London, have demonstrated that businesses are not immune from disaster. Yet research conducted by the London Chamber of Commerce and Industry in 2005 amongst South East firms revealed some alarming statistics in relation to contingency planning, disaster recover and business continuity.

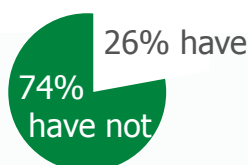


SMALL FIRMS



RETAILERS

These statistics are alarming, particularly as in May 2006 65% of London firms still believed another attack like 7/7 was inevitable. In addition, three quarters of company directors in the capital believed that London's transport network was no safer than it was before the 2005 bombings. Companies in the capital have failed to learn the lessons of 7/11 and 7/7, with many now less prepared to withstand a major incident. The proportion of all firms with contingency plans in place had fallen from 46% to 41%.



PLAN POST 7/7

So ask yourself the following:

Do we have a plan for?

- Contingency
- Disaster Recovery
- Business Continuity
- If so when did we last review the plan? Is it current?
- Does it comply with BS7799* or another external body?
- Who owns the plan?
Who is responsible for implementing it?
- What are our critical success factors for each plan?
- Who knows we have a plan?
- What expertise can I use to build our plan?

CONCLUSION

At some time in the future you will face the challenge of recovering from a security incident. How you respond when it occurs will determine your ability to trade in the future. We recommend that you develop a continuity plan that is structured, involves your people, has been tested and fully utilises the skills of modern day security best practice.

FURTHER ADVICE

A wide range of advice on business continuity is available and much of it is free. The Government's Preparing for Emergencies website www.pfe.gov.uk provides extensive information for businesses, including the booklet 'Expect the Unexpected'. This booklet is jointly published by the police National Counter Terrorism Security Office, London First and the Business Continuity Institute. More detailed advice for business continuity professional can be found at www.ukresilience.info.

The London Chamber of Commerce and Industry has also published guidance for businesses on how to draft and implement a business contingency plan, entitled 'Crisis Management and Business Continuity Planning: A programme for Business Survival' (see www.londonchamber.co.uk).

USEFUL WEBSITES/ REFERENCES

www.ukresilience.info
www.citysafe.org
www.londonchamber.co.uk
www.pfe.gov.uk
www.projectgriffin.org.uk
www.projectgriffin.org.uk
www.nactso.gov.uk

* BS7799 is a standard setting out the requirement for an Information Security Management System. It helps identify, manage, and minimise the range of threats to which information is regularly subjected.

In the first instance a risk impact assessment should be undertaken, which lists potentially serious incidents that would affect the operation of your company. The plan should include a list of events and the probability of their occurrence. The plan should focus on addressing those events with the highest occurrence probability and maximum potential impact. This will help define the plan in relation to the true needs of your company in an emergency situation.

The plan should have three main parts:

1. The security of your business

- How you intend to protect your people.
- How you intend to safeguard your strategic/key assets and infrastructure.
- How you can assist and coordinate emergency services on the ground.

You will need to agree with senior management the company's appetite for risk. You can then decide which risks can be accepted, which risks can be reduced and which risks should be managed using business continuity planning.

2. Roles and responsibilities

All plans look different but they should be clear about roles and responsibilities. You will also need to determine:

- The training required by the plan.
- What internal resources you will need.
- What external support you may need to bring in when an emergency occurs.
- What the process is for obtaining that resource.
- The role of your security officer in the event of an incident.

Suggested roles are:

FIRE

- Fire Warden / Marshals
- Evacuation
- First Aid
- Assembly point co-ordinator

POWER/WATER/UTILITY CUTS

- Emergency services call out
- Transfer to back-up power
- Restoration of Power
- Evacuation
- Centre of knowledge of building layout and service outlets
- Knowledge of key contacts/key holders

EXTERNAL THREAT

(Crime, terrorist attack, industrial espionage)

- Major incident liaison e.g. Project Griffin (see overleaf)
- Emergency services call out
- Evacuation

3. Critical success factors

- What they are?
- How to measure them?

TESTING YOUR PLAN

When the time has been taken to develop the plan it must be proven by testing it. Use rehearsals to ensure the plan can be implemented and that it will protect your business. Where possible involve external bodies including the Police in your testing. Any rehearsal should be conducted by the people you want to use in the plan (including your security officers) to familiarise them with their responsibilities should the plan ever be put in to effect. Make sure that your testing procedures are recorded and documented to continually fine tune the plan.

To cope with the ever changing security threats to your business, make sure your plan is regularly reviewed and kept up to date. All changes must be fully tested and personnel should be made aware of changing procedures and responsibilities.

It is extremely important to make all of your staff aware of your contingency plan and to ensure that they take it seriously, as lives may depend on it. Ensure that the plan is a key component of your training programme and involve your HR department in the delivery of training.

ROLE OF YOUR SECURITY PROVIDER

Your security provider should be instrumental in helping you to assess risks, vulnerabilities and potential impact. They should also be able to provide advice on integrated systems which can help you to reduce risk, eg controlled access systems to prevent intruders entering your buildings. If you have any questions about these issues please contact GBSG for further advice.

ASSIGNING KEY PERSONNEL

Make sure that the people you have assigned to tasks within the plan are able to operate in the most effective way when a security breach occurs.

Some businesses allocate the removal and transit of valuable assets, (patents, microchips, passwords, logs) to its security officers during a fire. Another good example of this practice is where businesses store system back up devices on the same premises. Based on their continuity plan, manned guards are given the responsibility to move back-up devices to a safe place in the event of a fire. In the event of a fire in an art gallery, security officers may, depending on the gallery's continuity plan:

- Remove all works of art.
- Direct firemen as to which articles to protect or remove.
- Prioritise the items to remove based on their assignment instructions.

Do you have the right people in place to handle an emergency situation effectively?