These critical issues papers are short briefing papers that describe to managers critical security issues, their background and the range of options there are for countering them. They are not technical in nature, but provide sufficient technical insight to enable a business manager to engage effectively with the information security professionals in the organization.

These briefings are therefore also effective tools for information security professionals who want to ensure that their managers fully understand a specific information security issue.
EXECUTIVE SUMMARY

Business continuity and disaster recovery planning are essential governance tasks for every organization. While the number of organizations whose sites and operations are likely to be specifically targeted by terrorists (the ‘Critical National Infrastructure’ or ‘CNI’) only numbers, in any significant first world country, in the low hundreds, ALL organizations are exposed to the indirect impacts of terrorist attacks.

Every organization should have a tried, tested and maintained plan that ensures that it can continue its critical operations while coping with the aftermath – both direct and indirect – of a terrorist attack. Those organizations that already have business continuity plans should ensure that their provisions for dealing with terrorism are up-to-date; the 30% of organizations that don’t yet have a business continuity plan need to put one in place as fast as possible. Terrorism is designed to create destruction and chaos; only a rehearsed, tested and detailed continuity plan can help individual organizations counter terrorist attacks.

BACKGROUND

A CBI/QinetiQ survey, carried out with MORI in 2004, focuses on those security incidents that are terrorism related. It reported that 32 per cent of organizations are most worried about direct terrorist action or terrorist incident, 20 per cent by environmental terrorists and 17 per cent by interruption due to a terrorist act.

Eliza Manningham-Butler, Director General of the UK’s Security Service, said this at the UK’s 2004 CBI annual conference:

“A narrow definition of corporate security including the threats of crime and fraud should be widened to include terrorism and the threat of electronic attack. In the same way that health and safety and compliance have become part of the business agenda, so should a broad understanding of security, and considering it should be an integral and permanent part of your planning and Statements of Internal Control; do not allow it to be left to specialists. Ask them to

www.itgovernance.co.uk
Page 2 of 10
Critical Issues 2: Terrorism & business continuity

report to you what they are doing to identify and protect your key assets, including your people.”

Cyber-terrorism

Cyber-terrorism is a far lesser threat than physical terrorism, even though cyber-terrorism has received substantial newspaper and political coverage over the period since 9/11. Cyber-crime is a significant risk; viruses, worms, Trojans and so on, all cause significant loss to unprepared organizations, but they are criminal acts without obvious terrorist intent. Joshua Green’s online article, The Myth of Cyber-terrorism, explores the reality of the cyber-terrorist threat. Nevertheless, all organizations should have appropriate arrangements to identify and report electronic attack incidents. In the UK, the advice of the NISCC (National Infrastructure Security Co-Ordination Centre) and its computer emergency response team should be taken into account. All developed countries have their own Computer Emergency Response Team (CERT) and, as a default, the US CERT site could be used for advice.

Nature of business continuity threats

All organizations face business continuity threats. This paper’s purpose is not to provide comprehensive business continuity advice, but rather to focus on the specific threats to business continuity created by terrorism.

Business continuity planning follows a standard process, which starts with a business analysis, a threat and risk assessment, a business impact analysis and then follows through with the creation, documentation and testing of a plan to deal with the identified risks.

Business continuity risks fall into four broad categories:

- Acts of Nature (fire, flood, storm, etc)
- IT or infrastructure failure (power or telecommunications system failure, etc)
- Industrial unrest or civil disorder
• Terrorism (international terrorist networks or sleeper cells, nationalist terrorists, anarchists, radical groups, etc)

A business continuity plan needs to consider how risks in all these categories might affect the business, with particular consideration of the likely impacts if a number of risk types co-occur: a terrorist attack that takes place during a violent storm in a period of civil disorder will create different challenges than one that occurs on a normal business day.

THE CRITICAL ISSUE

Terrorist attacks are an ongoing risk for all developed societies. Small terrorist groups – particularly in the last forty years – exploit democracy and capitalism in order to attack democratic, capitalist societies. There is no indication that the attractiveness of terrorism as a method of communication will lessen in the years ahead. Attacks are becoming more sophisticated, more destructive, and more random in their targeting of innocent people. Increasingly, they also have an economic objective: to disrupt the workings of the capitalist economy and cause economic dislocation, damage and loss. Disruption, for instance, of transport systems creates widespread shock and damage, which is one of the reasons they’re targeted.

Societies have to become increasingly resilient if they are to survive, and this resilience is dependent – to a significant extent - on the quality of organizational business continuity and disaster recovery plans, and planning processes.

DEALING WITH THE ISSUE

Business continuity plans need thorough preparation if the organization is to cope with the direct and – more often – the indirect impacts of a terrorist attack. There is an international standard of good practice for the creation, testing and maintenance of business continuity plans: PAS 56

Risk assessment

The starting point is a risk assessment.
There are two possible types of terrorist attack that the organization should consider: direct and indirect. Those organizations that face the possibility of direct terrorist attack are likely to be part of the CNI and should already have very specific business continuity plans in place. There are, however, many other organizations that are not part of the CNI but which could, because of a specific event, become the target of a direct attack. Events such as a visit (particularly one that has a high profile and has been well-trailed in the press and elsewhere) by a senior or international politician, a royal or by any other high profile individual, could increase the likelihood of a terrorist attack.

For most organizations, however, the real risk is in the indirect risk. This occurs when your organization’s premises or operations are damaged by an attack on another, adjacent organization, as the result of an attack on or during a local event, or the result of an attack elsewhere that has impacts on your customers, suppliers, staff or operations.

**Business Impact Analysis**

MI5’s [website](http://www.itgovernance.co.uk) identifies the following possible impacts that a major terrorist incident could have – in additional to commercial impacts – on any organization:

- damage to buildings, perhaps making them unavailable for a long period;
- loss of IT systems, records, communications and other facilities;
- unavailability of staff because of disruptions to transport;
- loss of staff (including key people) through death, injury, or unwillingness to travel;
- adverse psychological effects on staff, including stress and demoralization;
- disruption to other organizations or businesses – suppliers, outsourced service companies, professional advisers - on which you depend;
- damage to reputation;
Critical Issues 2: Terrorism & business continuity

- Changes in the demands – both external and internal - placed on the organization.

Other disruptions may be possible, including:

- Unavailability of staff due to police cordons preventing their access to work places;
- Unavailability of emergency services to deal with local emergencies because they are already overstretched dealing with the terrorist incident;
- Failure of telecommunications services, either as a result of the attack itself or through system overload;
- Failure of power services as a consequence of the incident.

Every organization should carry out a comprehensive assessment of the specific impacts that a terrorist incident may have on its own operations, ensuring that the disruption scenarios allow for worst case possibilities. This assessment should, nevertheless, be practical and realistic, because the likely costs to the organization set the limit to the appropriate amount that should be committed to dealing with the impacts. The fact that these costs are both indirect and difficult to assess doesn’t mean that an attempt shouldn’t be made to calculate them.

Planning issues

Business continuity planning points that are relevant when preparing to deal with the impacts of terrorist attacks should include:

- Interlinking with the business continuity plans of neighboring organizations to ensure that the local area is rationally used between you and that, wherever possible, you cooperate in responding to and dealing with continuity threats. Local authorities, partner organizations and emergency services should all contribute to your planning process, just as you should consider contributing to theirs.
- Clear, unequivocal guidance on steps that should be taken in specific circumstances – but guidance which is not so detailed as to delay an appropriate response.
Critical Issues 2: Terrorism & business continuity

• A contact and communications plan that allows for the possibility that mobile phone networks might be inaccessible, either as a direct result of the terrorist attack or because of user overload; pre-arranged contact and information points for members of staff and contractors working remotely should be pre-arranged so that, under all circumstances, it is possible to tell remote workers what is going on and what they should be doing;

• A planned calling tree – with all necessary contact details (which are kept up to date, for changes to staff as well as to their contact details) that enables the organization to make contact, under all circumstances, with all those people it needs to contact, including board members, staff, key customers and suppliers. These arrangements can include e-mail and telephone, will need to be appropriately staffed and will need to be capable of operating in disrupted and difficult circumstances. This calling plan should include provision for contacting people outside normal working hours, as well as those who might be abroad or on holiday.

• An emergency response team that has pre-arranged meeting places (at least two, one of which is at a distance from the first and capable of serving as a fall-back in case the first planned site is unavailable) and plans that will allow for one or more of the team members to be uncontactable – for whatever reason.

• Clear descriptions of who is to exercise what authority under what conditions, with prior information to everyone who might be affected as to what these arrangements are.

• Provision for receiving news, which might include a battery-operated radio (with fresh batteries) and/or a television set.

• Provision for helping staff get home, or for finding alternative, temporary accommodation at times when the public transport system is disrupted; advance arrangements with local hotels are amongst the options that should be explored in this regard.
Critical Issues 2: Terrorism & business continuity

- There should be arrangements for staff to work from home, which should include measures to equip, supervise and communicate with them throughout a period during which it is not possible to get into work;
- There should be arrangements for helping staff contact relatives and family members who, elsewhere, might have been exposed to the terrorist attack, or to its repercussions and aftermath.
- Appropriate plans should be made for counseling traumatized and bereaved staff (including circumstances of both local and a distant atrocity) and others who may be on the organization’s premises.
- Trained first aiders, together with their deputies, should be in place and particular care should be taken to ensure that there is adequate cover during holiday periods and times when the office is understaffed.
- Access to sufficient people with the expertise and motivation to lead and manage the organization through and beyond the crisis. This planning item requires that you give consideration to the possibility that senior directors may – for any one of a number of reasons - be unavailable at the time of crisis, and that redundancy and fall back options need to be considered. All plans should be rehearsed under circumstances that assume that at least the first and second in command in any area of the business is suddenly unavailable.
- Access to key records (financial, operational and personnel) as well as IT and communications systems – and, in particular, access to all these resources from alternative sites, which might include specific backup sites and which might include arrangements for remote access from unspecified third party sites;
- Financial arrangements are critical; the organization must be able to carry on paying staff and key suppliers, and must be in a position to purchase essential assets and services without necessarily having normal purchasing and accounting facilities available. This means that account facilities and
acceptable authorization methods should be identified and agreed with key suppliers in advance.

- It is critical that the organization be able to respond to demands from the media – preparation for this aspect should include training more than one person to handle the press, and should include a number of pre-planned press briefings.
- Plans should be made, and rehearsed, for dealing with all other likely eventualities, including telephone bomb threats, suspicious packages, emergency evacuations and similar situations. These plans and rehearsals should include input from the emergency services and should allow for situations in which the emergency services are overwhelmed and unable to provide immediate assistance.

Testing

Untested business continuity plans are not worth the paper they are written on. Business continuity plans are only useful if they work, and there is no way of making them work unless they are regularly tested. Fire alarms are tested, as are fire evacuation procedures. Business continuity plans – particularly those designed to counter the effects of a terrorist atrocity – must be tested under all possible scenarios. While plans can be ‘bench tested’ (i.e. tested in a tabletop simulation) the important test is a simulated real-life one. This itself will require planning and co-ordination to create and carry through a large scale exercise and there are specialist companies who can help with this. It can, however, be managed internally, as long as a small team of senior managers are given carte blanche to stage and run an exercise in which all members of the emergency response team and others throughout the organization are given unexpected scenarios and challenges to cope with.

All equipment on which the plan depends should also be tested in circumstances as near to reality as possible.

At the end of an exercise, it is important that all the lessons – what went well as well as what went badly – should be analyzed and incorporated into a new and revised version of the plan.
Of course, a business continuity plan that is designed to deal with the impacts of a terrorist attack should be integrated into the organization’s overall business continuity planning framework and consistency with all other plans should be maintained.

**Other resources**

- PAS 56 Guide to Business Continuity Management
- BCM Toolkit
- The Definitive Handbook of Business Continuity Management
- www.itgovernance.co.uk/page.business_continuity