ProtectUK

Managing risk and business continuity

Original publication date
02/11/2020

1. Introduction

Managing the risk of terrorism is only one part of a manager's responsibility when preparing contingency plans. Such plans may be in response to an incident or event, either within or near their premises, which may inadvertently impact staff safety, public safety or disrupt normal operations. It is important that this is one person's function and responsibility. The governing body or board is ultimately responsible and must be committed to managing the risks and understand the consequences of ineffective management.

Strong risk management processes will anticipate and assess risks to the organisation. The risks should be mitigated through preventative measures such as 'target hardening', the training of personnel and an effective use of information security systems. Having worked on preventing the risk materialising, the organisation must still be ready to respond and recover from a business interruption, regardless of its cause. There are a number of phases in a response, which are summarised in diagram

Incident response

Incident response deals with the immediate impact of an incident. It is a relatively short-term phase that focuses on escalation and activation, making sure people and the environment are supported and made safe wherever possible.

Incident management (IM)

IM refers to how the organisation will manage the consequences of the business interruption at the

scene through command, control, co-ordination and communication. It covers who is in charge, how to keep stakeholders informed, escalation processes, co-ordination of resources and much more.

Crisis management

Crisis management is about your arrangements to manage strategic, complex and unprecedented events. It is rarely standalone and will require integration with other disciplines. An incident may require a crisis management response without the need for a business continuity plan activation. This may be, for example, in the event of major negative media attention about the business. In contrast, there may be a ‘creeping/rising tide crisis’ where a disruption, such an attack on an IT system, emerges and, if not managed effectively, turns into a crisis. The incident response arrangements must therefore be flexible enough to manage both an operational disruption, which may need to be escalated, and a crisis situation, which requires strategic leadership.

Business continuity and resilience

These are the arrangements you should develop in order to maintain critical and urgent business activities to how they were before an attack and what work your business must continue to do to survive the disruption from a terrorist attack. Consider a range of impacts that could disrupt your business, including the unavailability of your building (through loss of utilities or evacuation), people (colleagues and suppliers) and equipment (machinery and IT). Then plan how you would continue critical parts of your business during disruption.

Business continuity planning is essential in making sure that your organisation can cope with an incident or attack and return to ‘business as usual’ as soon as possible. An attack on a crucial contractor or supplier can also impact on the day-to-day running of the business, so will need to be included in the business continuity plan. This is particularly relevant for smaller operations that may not have the resources to withstand even a few days of financial loss. Make sure sub-contractors are included and a serious consideration to the principal contractors.

International Standards ISO 22301 Societal Business Management Security Systems and Guidance provides further information on the subject of business continuity plans, along with the Business Continuity Institute (BCI) GPG (Good Practice Guidelines).

Free practical advice is available from your local authority or from the Business Emergency Resilience Group, a Prince of Wales initiative or via the BCI website.

Other useful resources:

The completion of a Business Continuity and Resilience Checklist can help.

The following websites are useful for advice and training on resilience:

- Emergency Planning College Website.
- Business Emergency Resilience Group website.
- Cabinet Office website.
- Government Emergencies, Preparation, Response and Recovery webpage.
- Government Emergency Planning webpage.

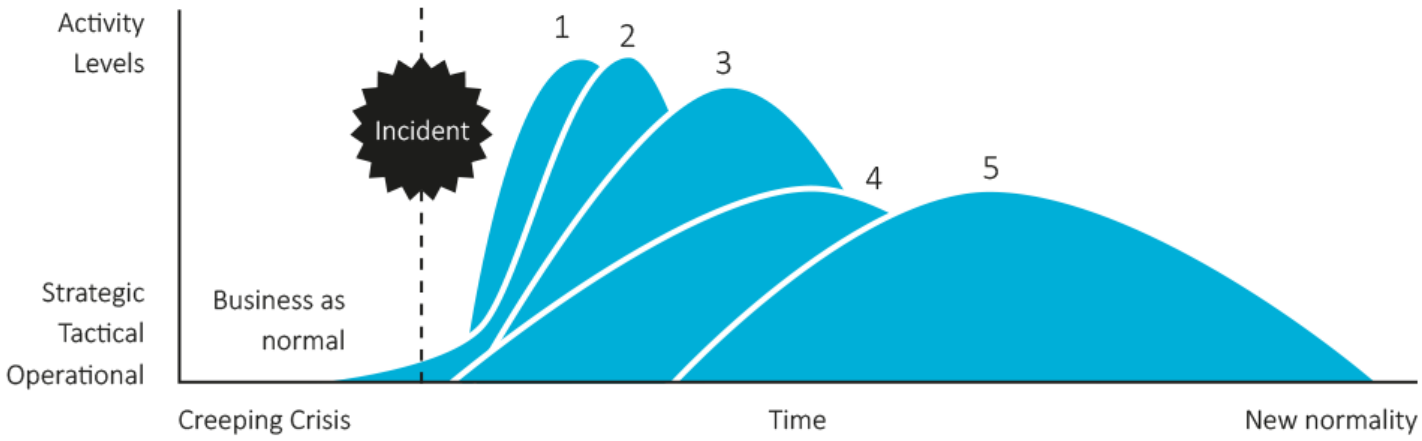
Business recovery

A business recovery plan usually takes place over a long duration, with wider stakeholder engagement and detailing the priorities for rebuild, recovery and restoration. It should detail how, and in what order, the return to the new normality following a disruption.

Response and recovery usually overlap – there is a transitional phase. After implementing the resilience arrangements, a formal debrief should be conducted in order to keep arrangements up-to-date.

Response activity over time:

- emergency services: response safeguarding life, protecting environment and company assets
- incident management: command, control, coordination, communication
- crisis management: strategic, complex and unprecedented reputation, stakeholder confidence
- business continuity: maintaining critical activities
- recovery: focussed on rebuilding, restoring and returning to business as usual



Risk management
prevention and preparation

2. Reputation

Failing to prepare for serious incidents may impact reputation and goodwill. Being resilience minded and better prepared reassures both customers and staff. Effective resilience could potentially deter or mitigate an attack.

3. Neighbours and partners

Do you know who your neighbours are and the nature of their business? Could an incident at their premises affect you? It is safer to communicate and work with those businesses around you.

A number of organisations have adopted good practice to enhance the protective security measures in and around their premises. This document identifies and complements such good practice.

This guide recognises that Publicly Accessible Locations differ in many ways, including size, location, staff numbers, layout, footfall and operation, and that some of the advice included in this document may have already been introduced at some locations.

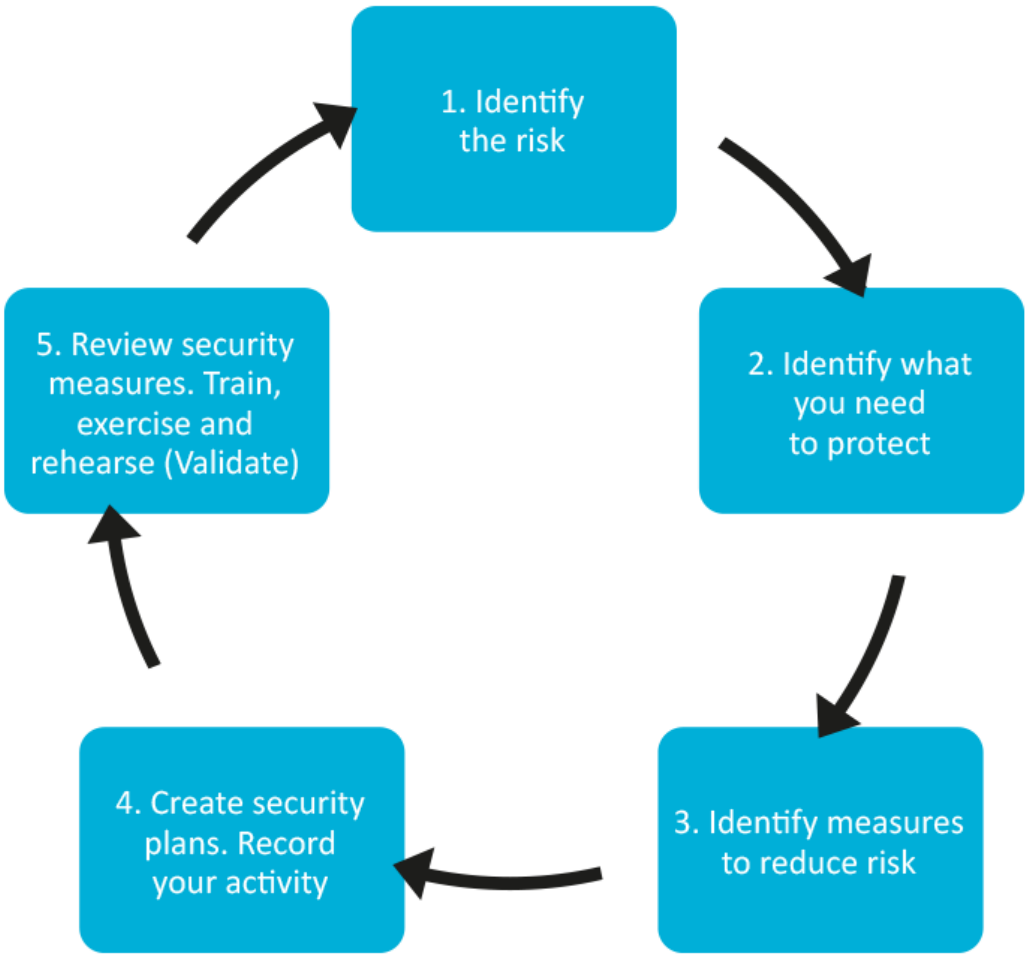
4. Managing the risk

With regard to protective security and resilience, the best way to manage the hazards and risks to a business is to start by understanding and identifying the threats, vulnerabilities and the resulting business impact.
This will help:

- what protective security and resilience improvements need to be made
- what type of security and contingency plans need developing

For some Publicly Accessible Locations, simple good practice, coupled with staff vigilance and well exercised contingency arrangements may be all that is needed. If, however, an assessment states the presence of an attack vulnerability, appropriate protective security measures should be applied to reduce the risk to as low as reasonably practicable.

The following diagram illustrates a typical risk management cycle:



Step 1: Identify the risk

Understanding the terrorist's intentions and capabilities, what they might do and how they might do it, is crucial to assessing risk. This guidance outlines in other chapters the threat and some of the current terrorist attack methodologies.

Ask the following questions:

- what can be learnt from the government and media about the current security climate locally, globally, or about recent terrorist activities?
- is there anything about the location of the premises, its visitors, sponsors, contractors, occupiers and staff, the activities, or within the wider community that may attract a terrorist attack?
- is there an association with high-profile individuals or organisations who may attract a terrorist attack?
- are there procedures in place and available for deployment on those occasions when VIPs attend your organisation? How often are the procedures reviewed? Are there resources and funding to support this as required?
- does the location mean collateral damage could be suffered as a result of an attack or incident at a 'high risk' neighbouring site
- what can the local police explain about crime and other problems in the area?
- are there any aspects of the business or activities, or those of staff, that terrorists might wish to exploit to aid an attack; for example, building floor plans, publicly available documents, technical expertise or poor security culture such as unauthorised access to restricted areas?
- is the information about the threat and building response levels communicated to your staff?
- are staff trained and advised to take a level of personal responsibility given the environment and threat of terrorism we face in society in general?
- are contracts with other companies restricted by the information they can publish online about you such as information or images of your site? For example floor plans, security features, patrolling detail etc.
- does anything identify vital installations or services critical to the continuation of business in the premises?

Read more about Digital Built Assets and Environments or go to the NPSA (formerly CPNI) website.

Step 2: Decide what needs to be protected and identify the vulnerabilities

Now that the risks have been determined, identify what needs to be protected. The priorities for protection should fall under the following categories:

- people - staff, visitors, customers, contractors, general public
- physical assets - buildings, contents, equipment, plans and sensitive materials
- information - electronic and paper data
- processes and policies - supply chains, critical procedures – the actual operational process and essential services required to support it.

For each, you need to consider:

- What is the vulnerability?
- Why is it vulnerable?
- What are they vulnerable to?

You know what is important to the business. It may be something tangible, for example, the data suite where all transactions are recorded, the IT system, or a piece of equipment that is essential to keep the business running. There are probably plans in place already for dealing with fire and crime, procedures for assessing the integrity of those employed, protection from IT viruses, and security measures to secure parts of the premises.

Step 3: Identify measures to reduce or mitigate the risk

Once what needs to be protected has been identified and why, understanding what measures the site has in place already, how effective they are and where the vulnerabilities are, follows. The measures you use should be proportionate, cost effective, and complement one another to produce an

integrated system.

An integrated approach to security and /resilience is essential. This involves thinking about physical security, cyber security, personnel security (such as good recruitment and employment practices) and personal security. There is little point investing in costly security measures if they can be easily undermined by a member of staff, supplier or contractor because poor recruitment and or procurement processes are in place. This guidance identifies and signposts measures which can be implemented to assist in mitigating the risks.

Remember, **terrorism is a crime**. Many of the security precautions typically used to deter criminals are also effective against terrorists. So, before investing in additional security measures, review what is already in place. There may already be a good safety and security culture on which can be built upon.

If there is a need for additional security measures, then make them cost-effective by careful planning wherever possible.

Introduce new equipment or procedures in together with building work. In multi-occupancy buildings, try to agree communal security arrangements.

Even if organisations or businesses surrounding your location are not concerned about terrorist attacks, they will be concerned about general crime; your security measures will help protect against crime, as well as terrorism.

Staff may be unaware of existing security measures, or may have developed habits to avoid them, such as short-cuts through fire exits. Simply reinstating good basic security practices and regularly reviewing them will bring benefits at negligible cost.

Go to the NPSA Operational Requirements webpage to learn more about your security needs.

Step 4: Create security plans

Security planning

Following a risk assessment, it is recognised that for the majority of Publicly Accessible Locations, the responsibility for the implementation of protective security measures will sit with a security manager or an assigned individual. They must have sufficient authority to direct the action taken in response to the risk.

They must be involved in the planning of the perimeter security, access control, glazing, contingency plans etc., so that terrorism is taken into account. The security manager must similarly be consulted over any new building or renovation work, so that counter terrorism specifications, such as glazing and physical barriers can be considered and factored in as appropriate.

The security manager at most Publicly Accessible Locations should already have responsibility for most, if not all of the following key areas:

- the production of the security plan based on the risk assessment.
- the formulation and maintenance of a search plan.
- the formulation and maintenance of plans dealing with, for example bomb threats, suspect packages and evacuation.
- liaising with the police, other emergency services and local authorities.
- arranging staff training, exercises, rehearsal, testing and exercising. Include their deputies and conduct briefings and debriefings.
- conducting regular reviews of the plans.

Creating your security plans

Effective security plans are those that are simple, clear and flexible. The security planner should call on staff with particular business area knowledge to help, such as an IT specialist, Procurement or HR manager (For example, this could help to consider countering the insider threat).

Plans should be:

- protective – the site search plan should counter the threat of a placed Improvised Explosive Device (IED), security patrols, deployment of CCTV, staff training etc.
- responsive – the actions which staff should take if they identify a person acting suspiciously, discover a suspicious item, receive a bomb threat, are the recipient of malware, or if there is a need to evacuate or invacuate. A communication and media strategy should also form part of this response.

The planning should include:

Policy	Be clear and document what you want to achieve
Operational	Put processes in place to make the policy to work
Physical	The "hardware" that supports any operational process
Education, training and awareness	Make sure those with a role to play in the security welfare of the site are properly educated and equipped to act confidently and effectively
Validation	Agree and implement appropriate measures to validate plans and arrangements. These may include exercises, tests or other techniques to establish the suitability, sufficiency and effectiveness of your arrangements
Partnership	Working with those who can or are needed to make security work
Review and monitor	Conduct regular reviews or following any change in circumstances such as a change in threat, circumstances, environment, post an incident or changes in
Communication and media	Identify how you will communicate with staff, visitors, suppliers and contractors

Action plans

To help progress security planning, it is good practice to create an action plan.

The action plan should set out:

- the activity to be undertaken
- a brief reasoning for the activity
- the name of the person responsible for completing the action
- a start date, review date and realistic completion date
- a scale to measure the actions progress, such as, red, amber or green

The action plan will form an important part of your security audit.

Step 5: review your security measures - train staff, rehearse, exercise and test security plans

Regularly review and exercise your plans to make sure that they remain accurate, workable and up-to-date. Additionally, consider reviewing plans if there is an attack elsewhere, or there is a change in threat or circumstance including to suppliers, contractors or stakeholders,. Through training, make sure staff understand their personal responsibilities, they accept the need for security measures and that security is seen as part of everyone’s responsibility; security is not merely something for security experts or professionals. Make it easy for people to raise concerns or report observations.
Rehearsals and exercises should, wherever possible, be conducted in conjunction with all partners, emergency services and local authorities.

Managing risk and security planning are on-going processes. Part of the validation process is to exercise plans and use any learning to further refine and make sure plans are workable to achieve the required outcomes.

The aim of your exercises should be to:

- make sure that plans work (verification)

- develop staff and third-party competencies and enable them to understand and practice carrying out their roles within the plan (training)
- test established procedures to make sure they remain valid (exercise, rehearse and validate)
- provide learning to further refine the plan (review)

Developing an exercise programme

The Business Continuity Institute (BCI) outlines five categories of exercising, they range in scale and complexity.

The main levels of exercise are:

1. Discussion-based exercises
2. Table top exercises
3. Command post exercise
4. Live
5. Test

BCI Good Practice Guidelines Training Course Module Six Version 1.0

Plan Review (Discussion based)	Table top/Command Post	Live play test
Very few resources are required, and can be entirely internal. No disruption to business or staff	More resources, planning and players are required. Can include external agencies	Significantly more resource intensive to plan and deliver
Can identify systematic issues in processes or gaps in processes/policies/procedures	Specific scenarios can be used and operational issues identified	Allows all staff and stakeholders to practice their roles/responses and identify issues that other exercise types do not
Does not address the effectiveness of processes, or	Virtual nature can lead to practical issues not being	Greatest level of realism, providing confidence that plans

Plan Review (Discussion based) allow staff to practice procedures	Table top/Command Post identified, and does not test reality	Live play test are likely to work in a real no-notice event

Remember: the greatest vulnerability to any organisation is complacency

5. Legal requirements

Management already have health and safety responsibilities under Health and Safety Regulations, the Civil Contingency Act 2004, and the Regulatory Reform (Fire Safety) Order 2005, or in Scotland, the Fire (Scotland) Act 2005 and Fire Safety (Scotland) Regulations 2006. The Management of Health and Safety at Work Regulations 1999 (the "Management Regulations") compliment the above legislation and set out explicit steps employers are required to take to manage and mitigate the health and safety risks present (or possible) in their working environments in line with the Health and Safety at Work Act.

As part of managing the overall health and safety of a business, reasonable steps must be taken to control the risks in the workplace. To do this consider what may cause harm to people and decide whether reasonable steps are being taken to prevent that harm. This is known as a 'risk assessment' and it is an exercise businesses are required, by law, to carry out. With fewer than five employees, there is not an obligation for a written record of this risk assessment. However, an assessment of risk must be carried out regardless and sensible measures to tackle those risks need to be implemented. Having identified any threats and vulnerabilities, the requirement is to assess how likely it is that harm will occur, i.e. the level of risk and what to do about it. Risk is a part of everyday life and you are not expected to eliminate all risks in their entirety, but rather, to manage the main risks responsibly.

Please note that independent advice in respect of the totality of your legal obligations should be sought.

6. Insurance

Insurance against damage to commercial buildings from terrorist acts is available but typically at an additional cost. Adequate cover for loss of revenue and business interruption during a rebuild or decontamination is expensive. Full protection against compensation claims for death and injury to

staff and customers caused by terrorism is also available, and again, will attract an additional cost.

7. Further information and advice

For independent and impartial counter terrorism advice and guidance that is site specific, the security manager should establish contact with the local police Counter Terrorism Security Advisor (CTSA).

The CTSA can:

- support you in assessing the threat, both generally and specifically
- give advice on physical security equipment and its particular application to terrorist attack methodology
- facilitate contact with emergency services and local authority planners to develop appropriate response and business continuity plans
- identify appropriate trade bodies for the supply and installation of security equipment
- offer advice on search plans etc.

It is also advisable to consult with other occupants, partners, stakeholder, neighbours, emergency services and the local authority.

ISO 31000, BS 31100 and ISO 31010 provide further guidance on risk management techniques.

KEYWORDS
RISK MANAGEMENT
RISK
INCIDENT MANAGEMENT
BUSINESS CONTINUITY
EMERGENCY PLANNING
PALS GUIDANCE