ProtectUK

Security risk management

ProtectUK publication date
14/03/2022

Why do you need to manage your security risks?

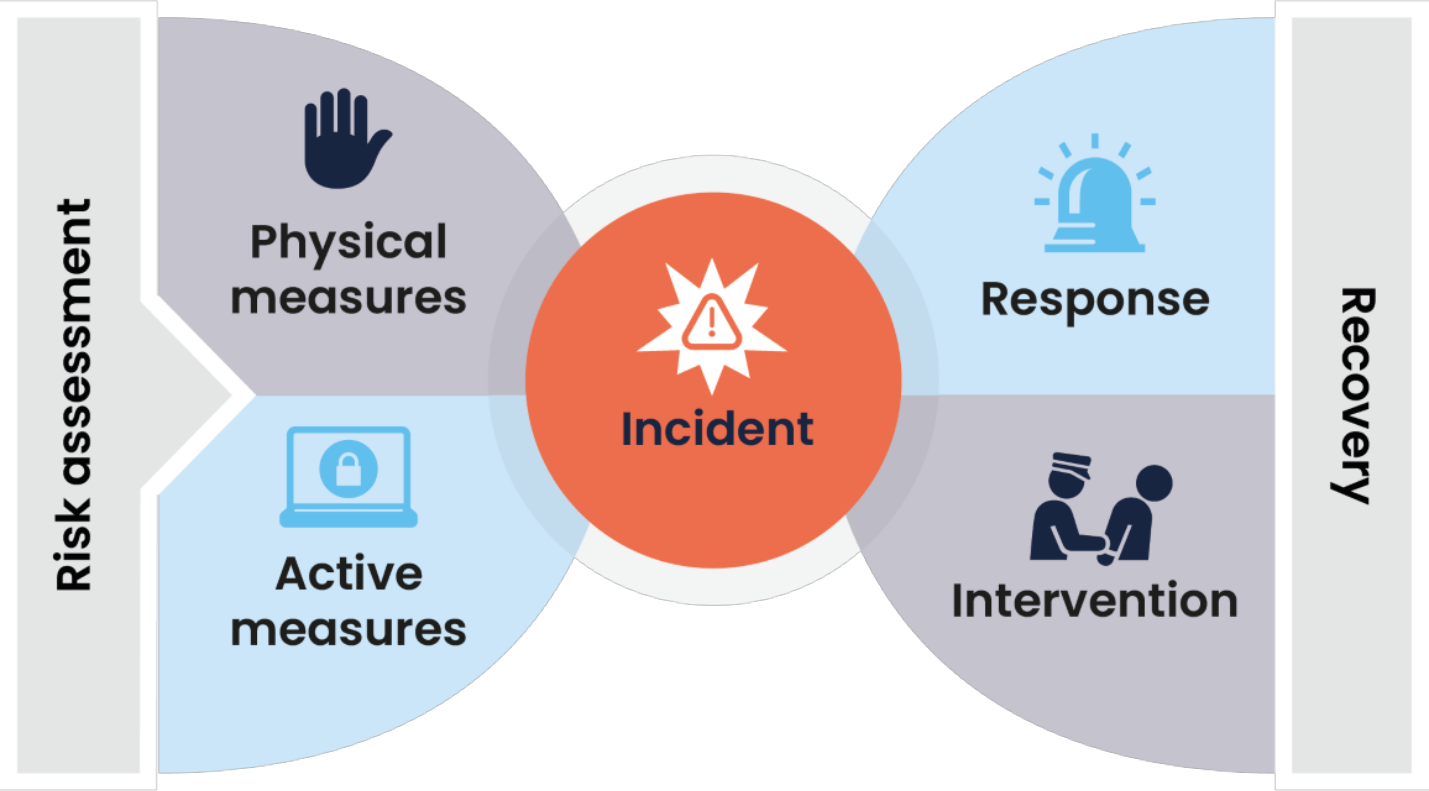
While it’s true you’re very unlikely to be caught up in a terrorist attack, as an employer, you are required by law to protect employees, customers, volunteers and other people visiting your sites, from harm.

If you’re unfortunate enough to be part of an attack, you need to have a system in place to identify and manage the risks. This will help your organisation to keep people safe and give confidence to those working in or visiting your site by showing that you have taken measures to protect them. This will also reduce the financial damage that might result from an attack and help protect your reputation or brand. It might also help you to manage other concerns, such as theft or safety.

Of course, having a system in place will be an important factor in any formal investigation such as an inquest, inquiry, civil claim or criminal prosecution.

This guidance provides information which will help you take forward a strong risk management system which will prepare your organisation to cope better if you should be caught up in an attack.

The Risk Management Model



The Risk Management Model explained

The diagram above has been adapted specifically for managing terrorist risk.

In this model, terrorist threats that the organisation faces, and the risks associated with these, are identified and assessed on the left-hand side of the diagram. These threats are shown pointing towards a possible security incident (such as an attack) in the centre. Between the threats and the incident are preventative measures of two types: **physical measures** and **active measures**, which protect the organisation from the threats before the event happens. However, it is almost impossible to eliminate all threats, so the right-hand side of the diagram identifies actions the organisation can take to reduce the impact or consequences of the threats after the event has happened. These also fall into two main types: **response** and **intervention**.

Finally, the right side of the diagram indicates that the organisation's security plan needs to consider how it will try to recover if an attack has taken place and harm has been caused.

1. Risk assessment

Risk assessment has two main components, the identification of terrorist threats and evaluation of the risks associated with these.

Identifying terrorist threats

Consider what sort of terrorists might be active in your location, who might carry out an attack and what types of attack you might face. Remember, although your organisation may be a very unlikely target for an attack, there may be businesses, organisations or sites nearby that might be attacked.

Look at your workplace and its location and think about why it might be attractive to a terrorist and what types of terrorist threats you might be exposed to:

- What is the threat level nationally and, if known, for your business sector?
- Are there any reasons why you or your neighbouring organisations may be deliberately targeted by an attack?
- Is there any reason why you or one of your neighbouring organisations would be easy to attack?
- Are there any events or other activities happening in your location which might attract an attack?
- What attack types may be used against your organisation?
- What work practices exist which may protect you from, or expose you to, terrorist attacks?
- Is there anything on your site which could be used to aid an attack (such as fuel stores)?

Look back at previous terrorist attack records as these can help you identify less obvious threats. Take account of differences in location, sector and the size of your organisation and how this might affect the nature of the threats you may face.

Evaluating the risks to your organisation

Once you have identified the threats, how likely people could be harmed by different attack types and how serious this harm could be. Think about threats to life from different attack types, if and how these apply to your situation and how employees, contractors, visitors or other members of the public might be harmed both in the short term and the long term.

In determining the level of risk you face, there is a range of factors to take into account:

- Could an attack on other organisations have an impact on you?
- What attack methods are they likely to use and how likely are they to succeed?
- Who might be harmed and how?

Note: Just because you think you are unlikely to be a target doesn't mean that you won't be. It is always safer to plan for the worst.

When thinking about who might be harmed, consider vulnerable people and their needs. Some workers or customers may have particular requirements, for example young customers, new or expectant mothers and people with disabilities. These requirements may place individuals at a higher level of risk because the locations they are in are more vulnerable to attack. They may be more likely to be a target because they may have mobility difficulties, making it harder for them to escape or evacuate premises.

Also note that security risks may be different at different times. For example:

- The risk level may increase or the risks change at different times of the day or on different days of the week
- Different types of events might take place in different parts of your local area or within your organisation

It is important to be clear about these differences and which ones your assessment applies to and it may be necessary to carry out more than one risk assessment.

2. Physical measures

The left-hand side of the Risk Management Model shows that there are preventive measures you can use to help detect, deter and/or delay an attack. This can be done through either physical measures or active (procedural) measures or, preferably, both.

Physical security measures come in three main types:

- **Buildings and infrastructure** – this includes physical barriers such as bollards and fences, strengthening buildings and other structures by using reinforced glass and blast doors, and optimising the layout of the site such as creating safe spaces and escape routes
- **Search and screening equipment** – this includes devices such as x-ray equipment, metal detectors and chemical and explosives detectors
- **Technology and control rooms** – this includes equipment such as electronic access controls, passive CCTV (e.g. for recording only), intelligent CCTV and other detection, tracking and alarm systems

For most small and medium sized organisations, and even some large ones, the scope for introducing physical security measures will be limited. However, there are some questions which you should always ask yourself:

- How many entrances and exits are there?
- Do these have doors that can be opened or closed quickly, or have other ways of blocking them?
- Are there clearly marked routes through the site?
- Do you have emergency or security lighting? Will the structure of the site (such as windows, internal walls, etc.) withstand or help protect against attacks?

3. Active measures

Active (procedural) security measures are concerned with what people on site do and how they do it to help prevent attacks.

Three types of people and their roles need to be considered:

- **Security personnel** – this includes guards and other security staff who patrol the site, search and screening staff, control room staff and other staff working in support roles with security, such as HR staff involved in recruitment
- **Front-line staff** – this includes any member of staff whose main role involves contact with customers, clients or visitors and who need to know what to do should an incident arise
- **Members of the public** – this concerns providing information and guidance to people visiting your site on how to protect themselves should an incident arise or to recognise an attack is under way. This can include various types of communication such as posters, announcements, signs, etc.

Not everyone listed above will be relevant to every organisation but some will be relevant to all organisations. The key is, what sort of actions are each type of person expected to take for you?

There are various questions you need to ask yourself:

- Do you use screening or searching processes before people enter your site?
- Are staff required to carry identification and is their access to your site controlled?
- Do you employ guards or other security staff and are they easy to identify?
- Are staff trained in observing, detecting and responding to terrorist threats?
- Do you have other forms of detection in place (for example CCTV)?
- Do you have a public address system?

4. Incident

The basic assumption is that an attack can happen and that this will have consequences even if the attack is not successful. The main considerations are the types of attack, the consequences and the responses to the different types.

No matter how good your preventive security measures are, it is not possible to stop all attacks or all the consequences of attempted attacks. Therefore, you need to be alert to what the consequences of an attack might be and how you might respond to and recover from an attack. For most organisations, this is where they have the most responsibility for their own actions. The starting point for this is thinking about the nature of the attack and how this affects both the consequences and the types of response you can make.

Attack types

The following are the types of attack most often used by terrorists in the UK. Some are much more likely and have more severe consequences than others depending on your organisation and circumstances. Your task at this stage is to decide which attacks you are exposed to and which could result in significant harm to individuals, your business or your organisation. The following list is roughly in order of how likely they are to occur:

- Marauding attacker (carrying a firearm, blade or other weapon)
- Vehicle as a weapon (primarily road vehicles but could be rail, shipping, aircraft such as drones)
- Improvised Explosive Devices (which can be carried, placed, posted, vehicle borne)
- Fire as a weapon
- Chemical, biological or radiological attacks (poisoning or other harm by chemical, biological or radiological means)
- Cyber-attack (when used to harm people, through controlling or disabling equipment or other devices and endangering safety).

Note: There are a wide range of less likely possible types of attack to think about, including kidnapping or hostage taking.

The key issues with all types of attack are: their most likely consequences, the amount of harm

caused, the timescales over which the consequences unfold, and how best to respond and recover from the attack.

5. Response measures

These refer to the immediate responses carried out by your organisation. Immediate responses can include:

- alarms and warnings
- RUN HIDE TELL actions
- evacuation procedures
- invacuation procedures (that is, separating your staff, customers, etc. from the attack within your own site)
- the use of first aid and fire protection equipment

In all cases, you should have a plan in place which includes training of staff, communications and practice drills.

The sorts of question that you need to ask yourself are:

- Do you have evacuation plans, invacuation plans or lockdown procedures in place?
- Are staff trained in operating these plans?
- Do you run practice drills or exercises to rehearse these plans?
- Do you have fire safety equipment, first aid kits and trauma kits readily available? Are staff trained to use them?
- Do you have collaborative arrangements in place with other organisations in your support network, such as neighbouring businesses, resilience units, local authorities and other security partners?

6. Intervention

Intervention refers to actions taken by the emergency services, and how your organisation can help them. Your organisation's role in an intervention includes: contacting the police and, when appropriate, other emergency services; working with and assisting the emergency services when they are on site; and taking actions when requested which require specific local knowledge of the site, such as turning alarms off or on.

Note: Once the emergency services arrive they will take full charge of the situation, and although they may request information or help from you, they are more likely to ask you and your staff to keep out of the way.

The sorts of questions you need to ask yourself are:

- Do you have communications and reporting procedures in place?
- Do you have established contacts to the police and emergency services?
- Are you able to brief the emergency services during an attack?
- Do you have easy access to potentially useful information such as floor plans, keys or access codes?

7. Recovery

Recovery can include processes for maintaining your organisation's activities after an attack, protecting your financial position following any harm or disruption and maintaining your organisation's reputation or brand.

The sorts of questions you need to ask yourself are:

- Do you have insurance cover for terrorist attacks?
- Do you have a business or organisational recovery plan?
- Do you have a business or organisational continuity plan?
- Do you have a media communication strategy?

Further reading

Recommended general guidance

- Protective security risk management
- NPSA - Protecting against terrorism (formerly CPNI)

Recommended specific guidance

Risk assessment

- NPSA - Recognising terrorist threats (formerly CPNI)
- National stakeholder menu of tactical options

BowTie Model explainer:

BowTie: a visual tool to keep an overview of risk management practices

Physical measures

- Publicly accessible locations - Physical security
- NPSA - Physical security (formerly CPNI)
- Secure by design link

Active measures

- Protective security measures

Incidents

- Marauding terrorist attacks
- Mi5 - Terrorist methods

Response measures

- Publicly assessible locations - Threat level and building response plans
- NPSA - Improving organisational response (formerly CPNI)

Recovery

- Publicly accessible locations - Managing risks and business continuity
- NPSA - Business continuity (formerly CPNI)

Please note this list is not exhaustive and does not cover all the relevant legislation which may apply.

KEYWORDS

RISK MANAGEMENT
RISK ASSESSMENT
RISK
SECURITY MEASURES
ATTACK

PAGE CATEGORY

SECURITY RISK MANAGEMENT