Revo

Retail. Property. Community.

Security threat mitigation Response levels.

Guidance note 95

Revo would like to thank NaCTSO, Intu, Westfield Europe Ltd and the Revo Security and Safer Shopping Committee for their help in developing this guidance note.

Section 1:
An overview of security threat levels, attack types and response levels.

This guidance note outlines all the different security threat levels and allocates an appropriate response level to each of them. It then provides detailed instructions on what to do at each response level and clarifies the different types of attack a shopping centre may be faced with.

Please note that this guidance note supersedes the advice contained within BCSC Guidance Note 48 dated February 2007.

Introduction.

Terrorism threat levels are designed to give a broad indication of the likelihood of a current terrorist attack. They are based on the assessment of a range of factors including relevant intelligence, capability and intent of potential attackers. This information may be incomplete and decisions about appropriate security mitigation measures should be made with this in mind. The measures listed in this document are not exhaustive. They are meant to aid your thinking in developing your own bespoke mitigation response level policy.

In particular, shopping centre owners and management are reminded that an attack might occur without warning. Therefore day-to-day security risk mitigation measures must be proportionate and cost-effective.

Threat level definitions.

- **Critical** – an attack is expected imminently
- **Severe** – an attack is highly likely
- **Substantial** – an attack is a strong possibility
- **Moderate** – an attack is possible, but not likely
- **Low** – an attack is unlikely

Attack types.

Non penetrative vehicle attack: the use of a parked vehicle to deliver an explosive attack. The attacker(s) will seek to get the vehicle as close to the site as possible in order to achieve maximum injury and damage. This may be achieved through encroachment, deception or duress. The attacker(s) will seek to evade detection.

Penetrative vehicle attack: the use of a vehicle as a weapon itself or the use of a vehicle to deliver an explosive attack by penetrating the site perimeter or fabric of a building / structure. The attacker(s) will seek to get the vehicle as close to the site as possible in order to achieve maximum injury and damage. This may or may not be a suicide attack.

Person borne improvised explosive device (PBIED): a suicide attack in which the attacker(s) wear or carry an improvised explosive device.

Improvised explosive device (IED): an improvised explosive device that is placed or secreted at a site. The device may be carried in any type of container, such as a bag or rucksack to avoid detection.

Postal IED: an explosive item delivered through the postal system including hand delivery and delivery by courier. The contents may include an improvised explosive device or hazardous substance i.e. a 'white powder' threat.

Marauding terrorist firearms and weapons attack: an indiscriminate attack against people by single or multiple attackers using firearms or other weapons. Attacker(s) may or may not use IEDs or PBIEDs.

Response levels.

Response levels should be designed to mitigate security risks. It is important to define what risks are being mitigated before delivering and what might be extremely costly protective security risk mitigation measures. On occasions, the least expensive and easiest to deliver security risk mitigation measures have the greatest effect.

There are three response levels that broadly equate to the threat levels as shown below:

Threat level	Response level
Critical	Exceptional
Severe	Heightened
Substantial	Normal
Moderate	Normal
Low	Normal

An overview of security threat levels,attack types and response levels.

The security risk mitigation measures applied at each response level will depend on various factors including amongst many other things, the location of the site and the existing risk mitigation measures in place.

Response level definitions.

Normal
Routine baseline protective security measures, appropriate to the business concerned.

Heightened
Additional and sustainable protective security measures. These reflect the broad nature of the threat, specific business and geographic vulnerabilities and judgments on acceptable risks.

Exceptional
Maximum protective security measures to meet specific threats and to minimise vulnerabilities and manage risks. Extra measures implemented are likely to sustainable for a limited period only.

Section 2:
The response level checklist.

The following good practice checklist is intended as a guide for shopping centre owners and management to assist them in identifying the hazards and risks associated with counter terrorism planning. It is not exhaustive however some of the guidance might not be relevant to all shopping centres.

The following factors should be taken into account when reviewing security risk mitigation:

- What is the threat?
- What protective security risk mitigation measures are in place currently?
- Have you consulted your local counter-terrorism security advisor, local authority and/or emergency services?
- What is appropriate and relevant for your shopping centre?
- Who else should be consulted? (business crime reduction partnerships, significant neighbours, occupiers, etc.)
- Which measures can be implemented easily?
- Which measures will take greater planning and investment?

Normal response level.

General security

- Maintain established security patrolling/manning of malls, common areas, car parks, cash handling, and assist retailers as required.
- Maintain established, secure access control arrangements, e.g. the basement service, roads/areas, access codes to the centre management office (CMO) and other controlled areas both front and back-of-house.
- Maintain any electronic patrol manager systems.
- Hold regular liaison meetings with any Retailers Against Crime groups.
- Hold regular liaison meetings with local police.
- Carry out periodic security checks of all unoccupied properties, including adjacent properties.
- Devise and test range of search plans.
- Ensure all reporting systems are in place and up-to-date.

Physical/maintenance

- Carry out regular reviews and maintenance for all security equipment, e.g. CCTV, radio links, desks phones and mobile phones.
- Ensure regular inspections of critical plant areas.
- Carry out periodic fire alarm checks/inspections of all unoccupied properties (including adjacent properties) where appropriate.
- Regularly inspect and replace as necessary the contents of 'grab bags' and first aid boxes.

Administration and communications

- Regularly review occupier and management record lists with latest management changes.
- Regularly review retailer key holder lists.
- Conduct regular reviews and updates of details held within your crisis management plan (CMP), including the 'communications plan' section.
- Regularly check that all CMPs and associated documents are available and accessible in the control room, the general manager's office and the operations manager's offices.
- Ensure that security is regularly discussed at staff meetings to maintain awareness and highlight any recent appropriate developments/occurrences.
- Conduct yearly exercising/testing of your counter-terrorism attack type response.
- Test mass communication links with occupiers.

Heightened response level.

Ensure that all normal response level measures are in place before you consider delivering the following security risk mitigation measures:

Immediate actions

- Hold an immediate security meeting with the onsite police team if relevant.
- Immediately re-inspect contents of 'grab bags' and first aid boxes.
- Immediately inspect all security equipment, e.g. CCTV, radio links, telephones, and repair/replace as required.
- Conduct an immediate test of all established communication links and mechanisms.
- Immediately carry out review and update of management record lists and retailer key holder lists.

General security

- Increase frequency of internal and external security checks of vulnerable areas.
- Test and exercise search plans.
- Hold specific security awareness meetings ensuring staff and retailers are aware of assembly points and any alternative assembly points. Daily briefings of security teams should be in place with monthly security forums/scheduled meetings.
- During specific security meetings, re-emphasise the importance of reporting all suspicious incidents/occurrences.
- Tighten compliance with signing in and out for all visitors/contractors.
- Introduce random checking of all vehicles entering service/reception areas.
- Increase CCTV observation of all car park entry points and review ability your to respond to suspicious vehicles.
- Increase checks on customer lockers.
- Review opening/closing procedures to ensure easily implementation if required at additional times.
- Enact the standoff enforcement policy.
- Implement the deployment of the CPNI Deterrence Toolkit, back-of-house messaging for short periods.
- Enact the schedule for the irregular/ad hoc pre-opening and post-closing of premises search.
- Enforce all access control points.

Physical/maintenance

- Inform any occupiers' staff and sub-contractors of increased threat level.

Administration and communications

- Review delivery arrangements and the handling of post.
- Review operational rosters to ensure that there are additional resources available to increase staffing levels when appropriate.
- Contact security partners who can provide the support of additional security personnel if requested.
- Ensure all incidents are fully documented and all contact with emergency services is included in security reports.
- Introduce regular joint management security meetings.
- Review centre websites using the CPNI Security Minded Communications Toolkit.

Exceptional response level.

Ensure that all normal and heightened response level measures are operating before delivering the following:

General security

- Confirm the threat level with the police and inform them of the additional measures being introduced by your centre. Monitor the MI5 website, news channels, etc.
- Increase visibility and numbers of security personnel.
- Introduce high-visibility (hi-vis) coats/tabards for all security personnel.
- Consider the removal/sealing of waste bins.
- Seal and close customer lockers.
- Increase the frequency of perimeter and corridor checks.
- Increase the level/frequency of vehicle searches upon entry to service/reception area(s).
- Reinforce understanding of evacuation procedures and assembly points.
- Ensure that traffic control officers are rigorously maintaining all 'no parking' zones adjacent to centre.
- Restrict parking near key points and publicly accessible entrances.
- Enact pre-opening and post-closing of premises searches.
- Enact proactive highly visible and irregular premises/area searches during opening hours for suspicious items.
- Consider enacting random or targeted searches of persons entering centre.
- Consider a permanent management presence in the malls at all times.
- Cancel non-essential off site meetings.
- Ensure maximum deployment of staff in the malls at all times. Consider bringing in additional resources if required.
- Place staff on key entrances (including back-of-house entrances) and ensure they are highly visible to the public.
- Consider reducing number of public access/egress points.
- Regularly test the PA system. Prepare pre-set messaging that reminds the public to report any unattended baggage and suspicious behaviour to the customer service desks.
- Ensure that patrolling security officers/security supervisors have the keys to entrance doors. In the event of risk of incursion into the centre from protesters or threat to life outside the centre, a dynamic lock-down of the centre should take place.
- Implement CPNI Deterrence Toolkit for duration of exceptional response level to heighten staff awareness.

Physical/maintenance

- Raise the profile and numbers of cleaning personnel. Ensure that they are briefed in reporting of suspicious or unusual items.
- Increase cleaning/clearing regimes to ensure all areas are kept clear, clean and tidy.
- Postpone non-essential maintenance that will have an adverse effect upon the centre's security.
- Heighten the priority for all outstanding repairs/maintenance to all security equipment.

Administration and communications

- Ensure all management record lists and retailer key holders lists are updated and located in control room and the centre management office.
- Ensure all local contact numbers for emergency services are updated and located in control room and the centre management office.
- Enact mail screening procedures. You must do this if the threat is a postal attack.
- Increase the frequency of staff meetings with emphasis on security updates on all security matters, and that include personal security of staff.
- Review access control arrangements to management suite and limit visitors. Where possible, ensure that all visitors to the centre management suite are pre-arranged and that the host is contacted upon their arrival and they are escorted at all times.
- Introduce bag searching within centre management offices upon authorisation from head office and as per advice under search policy
- Enact daily joint management security meetings.

Section 3:
General guidance.

Vehicle borne attack.

Standoff enforcement policy for vehicles

Shopping centres have individual challenges in relation to vehicles and the potential security issues that they present. It is not possible to fully prohibit vehicles encroaching into the crowded place. Some shopping centres are city centre based and rely on local authority traffic enforcement solutions as part of their security measures. Some centres are classed as out-of-town so encourage vehicle parking close to the centre. All centres have car parks either as part of a multi-storey scheme or in external areas. These car parks cannot form part of the stand-off enforcement measures, as by their design, they allow vehicles to park as close to the crowded place as possible.

Specific attention should be placed around the public entry areas and entry areas where vehicle security barriers are in place.

Standoff enforcement

Proactive monitoring of CCTV and regular external checks of the centre must form part of the daily security routines. In the event that a vehicle is left unattended and / or is parked outside of a designated area, that vehicle must be treated as suspicious. CCTV should be used if possible to determine how the vehicle arrived at its location. The identity of the driver and vehicle occupants should be confirmed and this information should be used to determine how suspicious this vehicle is.

If it is confirmed that the vehicle remains suspicious, its details must be reported to the police using the 999 system immediately. Its full details should be passed with the report. The centre emergency management plan and crisis management process should be activated immediately.

Local authority engagement

Local authority engagement is encouraged to supplement the security measures in place across shopping centres. All centres should engage with their respective local authorities to gain an understanding of traffic management and enforcement affecting their centres. By understanding what plans are in place via the local authorities. Further assessments can be undertaken in reviewing the security measures for vehicle controls at the centres.

Hostile vehicle mitigation (HVM) measures

Some shopping centres have adopted HVM security measures in the way of PAS (Publicly Available Standard) 68 / 69 security bollards / barriers. Where these security measures are in place, regular assessments of these measures should take place. If these measures require a maintenance plan, this plan should be reviewed and records maintained.

HVM operational policy

Only authorised vehicles / persons must be allowed into secure areas which are protected by HVM measures in a loading bay / service road area. Confirmation as to the purpose of their visit is to be checked and recorded and detailed within the entry logs prior to entry being granted. Pre-authorised vehicles should undergo the same checks. Any person responsible for operating a HVM measure must have received the appropriate training and confirmation of this training is to be recorded on site. Regular reviews of this access control HVM policy should take place.

HVM operation

When active measures are deployed, they should be in the up right or engaged position. The HVM policy detailed above should be enacted and carried out.

There are five main types of vehicle-borne attack:

- Parked vehicles: an attack may come from a vehicle borne improvised explosive device (VBIED) in a parking area of unscreened vehicles which may be underneath or adjacent to a target.
- Encroachment: incomplete or incorrectly spaced counter-measures can allow a hostile vehicle to enter an area without the need for impact. A hostile vehicle may also be able to tailgate a legitimate vehicle through a vehicle access control point (VACP).
- Penetrative attack: the use of the front or rear of a vehicle as a ram to breach a perimeter / target premises in order to get a hostile vehicle closer to the intended target.
- Deception: various forms include use of stolen or cloned ID, verbal deception or a 'Trojan' (disguised) vehicle.
- Duress: duress imposed on the occupant of a legitimate vehicle to carry a hostile payload into a protected site or duress imposed on a guard to grant vehicular access through a VCAP.

Person borne improvised explosive device (PBIED) suicide bomber.

The following information acts as guidance on how to manage this type of incident. This being said, our advice is that no member of the shopping centre team should put themselves in danger. In the event that a suspected PBIED is in the centre police must be called immediately. The emergency plan must also be activated imminently.

- Confirm – the location and description of suspect and inform CCTV control room.
- Cover stay 50 yards away from the suspect at a point where it is possible to maintain visual contact. Keep the suspect on CCTV.
- Contact your supervisor and request more police assistance. Instigate your crisis management plan.
- Civilians direct them to a place of safety but not if this is likely to compromise or further endanger the public or other officers. Enact the centre emergency management plan.
- Colleagues prevent other officers coming into the danger area. Cordon off the area and consider evacuation.
- Check for further suspects or devices and maintain control until police arrive.

Improvised explosive device (IED).

Within the detailed security procedures at each centre there are detailed procedures for dealing with suspicious packages. In addition the following 'H.O.T principles' should be adopted:

H. Has the item been hidden?
Has any attempt been made to conceal it from view or to place it where accidental discovery is unlikely? Use CCTV to evidence how suspect package arrived at its location. Innocent items are not usually hidden deliberately. Because of the consequences of a device being found before it functions, explosive devices are not usually left out in the open.

O. Is the item obviously suspicious?
Does it look like a bomb? Does it have wiring, circuitry, a power supply or something else attached to it? Has it been found after a suspicious event? Has there been any intelligence to suggest that you could be the target of a bomb?

T. Is the item typical of what you might reasonably expect to find in the given location?
Does the item look like it belongs? If the item is deemed to be suspicious, follow the 5 C's:

- Confirm that the item does not belong to anyone
- Clear the area
- Communicate
- Cordon off the area:
  100 metre cordon – small items, e.g. rucksacks or briefcases
  200 metre cordon – medium items e.g. suitcases, wheelie bins, cars, etc.
  400 metre cordon – large items, e.g. vans, lorries, etc.
- C: control the area
- Do not use any radio or mobile phone devices within 15 metres of any suspicious item:
- create a rendezvous point (RVP) outside of the cordon distance with easy vehicle access and parking
- conduct a search of RVP for any suspicious items; and
- inform police of RVP location.

The centre premises search plan should also be undertaken to ensure that there are no secondary or supplementary devices.

If an evacuation is undertaken the following must be undertaken:

- you should not use your fire evacuation points. These may be within the cordon area and could prove easy places for the placement of a secondary device
- conduct a search of the evacuation point for suspicious items.

Housekeeping: these are the good practice processes to deter or detect placement of IED's. Examples to be included in the policy are the regular trimming of foliage, the regular emptying of bins and staff conducting a pre-opening and post-closing search of the premises.

Active search regime: this is deterrent and detection activity. Examples would include regular inspection of bins, foliage, toilets and all other areas and spaces where IED could be left / placed.

Deterrence tool kit: CPNI have developed a set of back-of-house communication materials, based on the security infrastructure, that cause terrorists to be concerned about being detected. The materials achieve this in two ways: creating the impression that the site knows what hostile reconnaissance is (what they are up to) and creating the impression that everyone is watching out for them. See the CPNI website for more information.

Security minded communications: corporate communications is a relatively untapped but potentially very effective layer of protective security which can be achieved at little, if any, cost. This guidance shows how corporate communications can help deter those seeking to carry out hostile reconnaissance; especially when they are trying to select their targets. It also shows how they can enhance and augment the deterrent effect of protective security. See the CPNI website for more information.

Staff vigilance campaign: employee behaviour is a key indicator of your organisation's attitude to security. Vigilant security behaviour, such as awareness of surroundings and engaging with strangers, will show any hostile individual watching that it's not just security guards and CCTV they need to worry about. Alert employees are just as likely to spot suspicious activity and report it. CPNI has developed an approach to help you instil vigilance behaviours in your staff, which in turn will help them become an active part of your protective security regime.

This guidance helps organisations understand what constitutes good and bad employee vigilance security behaviour and demonstrates how to communicate it to the workforce. It provides the tools to run a 'security-minded behaviour' campaign, including links to professionally designed supporting materials.
See the CPNI website for more information.

Postal device: it is not possible or practicable to scan all incoming mail delivered to shopping centres. Centre management is only responsible for accepting mail deliveries to the centre management suite. Individual retailers are responsible for their own mail and are responsible for ensuring that they have their own checks in place.

All employees responsible for dealing with letters or parcels received in their centre should follow the advice below. Where possible, the mail should be taken to a location outside of the main centre management suite area to undergo an initial screening check prior to delivery into the management suite.

General guidance.

It is difficult to identify an explosive device but any suspicious package should only be dealt with by trained experts. This being said, there are several characteristics that should be looked for:

- point of origin (a foreign, unusual postmark)
- crudely addressed (incorrect spelling, hand-written, incorrect titles or initials, etc.)
- uneven or lopsided weight
- excessive weight for size
- strongly packed
- marked "To be opened by", "Personal" or "Confidential"
- excessive thickness (for letters)
- protruding wires
- oily stains
- the smell of almonds.

In all of the above, the letter or parcel must be treated as suspicious and dealt with accordingly. The package should be isolated as much as possible. Do not:

- use a radio or a mobile telephone near the package
- use any machinery near the package
- start up any vehicles nearby
- pull wires
- place the package in water
- cover the package with sand or anything else
- shake the package
- squeeze package
- put the package in a box
- panic.

If you discover a suspect item and you are concerned that it may contain chemical, biological or radiological material:

- if the item is still intact, do not shake it, squeeze it or open it
- if it is an item of mail that you are already holding, place it in a transparent, sealable plastic bag or container
- if you do not have a container, cover it with anything to hand (e.g. clothing, paper, a waste bin, etc.) and do not remove this cover
- do not touch, tamper or move the suspect item elsewhere
- turn off all air conditioning, fans, photocopiers, printers, computers and heaters
- if the contents of the package have spilled on to your clothing remove that piece of clothing, close all windows, evacuate the room, close all doors and leave the keys in the lock. Do not rub your eyes; touch your face or other people. Thoroughly wash your hands in soap and water as soon as possible. Place, if practicable, a clearly visible warning on the door.

Go to an isolated room and avoid other people if you can. It is vitally important that you segregate yourself and others who may have come into contact with the package. Reassure your colleagues. It is unlikely that they are contaminated and they will get medical treatment if required. Get access to a phone. The emergency services may wish to speak with you directly. Where possible, nominate someone who has not been in contact with the package to meet and speak with the emergency services.

Marauding terrorism, firearms and other weapons attack.

The immediate priority is to get people away from the threat. All staff should see the Stay Safe 'run hide tell' video and all retailers should be encouraged to view it as it is the principles from this video that should be adopted.

General guidance.

Do	Do not
Be aware of the centres response plan to a firearms incident and know your responsibilities in respect of this.	Delay in contacting the police on 999.
Ensure that you have participated in a test response plan (the police will have been contacted to join in the exercise).	Panic.
Report and act on any unusual or suspicious behaviour. Utilise the information given during the hostile reconnaissance toolbox talk.	Release any CCTV footage to the media.
Ensure that the duty control room officer monitors CCTV for behaviour that would be a trigger for hostile reconnaissance.	Ignore any suspicious activity.
Ensure 'emergency action boxes' or 'grab bags' contain substantial medical equipment such as first field dressings.	Challenge the suspects.
In the event of a firearms incident call the police on 999 and clear the immediate area of all personnel to somewhere safe, without creating panic.	Make any comments to the media. All enquiries should be passed onto the company's PR agency.
The safety of shoppers and staff is of paramount importance. Evacuate the immediate area and consider evacuating the centre. Think about how you will do this without causing more panic.	
Inform the duty manager who should collect all the details to pass to the police on their arrival.	
There should be pre-planned 'safe routes out' through service areas. Retailers and security personnel must be aware of these.	
Retailers should be contacted and instructed to cease trading, close their mall shutters and doors, collect as many shoppers as possible inside their unit and remain out of sight.	

Cover from gunfire

This is identified as:

- substantial brickwork, steelwork or concrete which can provide shelter
- car engine blocks; this is only applicable if the vehicle is in a car park or if they happen to be on display in the mall
- earth banks and large trees (particularly in open schemes).

Cover from view

This is identified as:

- anything where people can hide and be out of sight from the gunman
- consider rooms out of sight of public view — storerooms, for example.

In the event that an attacker has entered the centre, adopt the Stay Safe 'run hide tell' approach. When it is safe to do so, provide the police with as much information as possible for example:

- how many subjects there are
- his / her / their description
- whether the weapon(s) has / have been fired or not
- whether the weapon(s) is / are rapid fire or not
- the best location to enter the centre from
- if the centre is the process of evacuation / invacuation
- the direction of travel of the subject(s) within the centre
- if the subject(s) has / have evacuated the centre.

The duty control room officer should monitor the situation on CCTV gathering as much detailed information as possible. This will allow you to build evidence and keep a detailed log of events. If possible, have separate staff overseeing CCTV, phones and the event-logging process. While this is happening:

- turn off all mall music
- approximate the numbers of members of public in the centre. Are they aware of the incident / of the subject?
- listen / look around to see if the fire alarm / sprinkler system has been activated
- find out if there have been any casualties. If so, find out how many and where they are located in the centre
- ensure you are available to provide live updates as to the shooters movements and actions within the centre
- stop bystanders recording the event on their mobile phones
- keep a log of events and use the CCTV to record the event
- approach witnesses if available and collect statements
- inform the company's PR agency. The duty manager should be the central point of contact for all media enquiries and other staff should be instructed not to speak to the press but to direct all enquiries to the duty manager
- pass all evidence requested to the police along with names and addresses of any witnesses
- once cleared to do so, repair any damage and clear up the area
- offer counseling to security officers and other members of staff involved in the incident.

Search policy

Shopping centres as public crowded places unfortunately cannot enforce strict searching regimes. While wanting to ensure the safety of the public visiting the centres, it is not practicable or possible to introduce regular searching regimes within public entrances to the malls. However, in the event that the threat level is raised to critical and the threat contains a higher risk to crowded places consideration should be given for the introduction of search regimes.

These searches on public entrances should be operationally determined at site level upon the authority of head office. Consideration should be given to reducing entrance and exits points within the centre. In addition, right of entry should be granted upon agreement to be searched. No personal searching should take place, only bag searching and emptying of pockets of outer garments, etc. Searching should be in place for a short period of time and as stipulated below, upon the authority of head office. In the service yard / loading bays random searching of vehicles should take place. Site-based teams should follow the search procedures detailed within their security instructions and relevant training should be provided.

Search regimes should be undertaken by trained staff and are designed to create opportunities to deter attack and detect threats. Regimes should be unpredictable in duration and location.

Searching: vehicles

Security officers have no automatic right to search and permission must be obtained by the vehicle driver before the search is commenced. In the event that the driver of the vehicle denies permission to be searched then they should be refused entry to the centre service road / loading bay area.

Vehicle searches will normally take longer than personal searches, so discretion should be used. Concentrate on only two or three specific areas of the vehicle, unless instructed otherwise. Ensure that the driver is present at all times and that they are asked to open boots, bonnets, rear doors, glove compartments, cases, boxes, packages, etc. This is to prevent any allegation of 'planting' property by the officer.

It is good practice to wear gloves and use a torch during the search. Always ask the driver to switch off the engine and if searching under the bonnet or in the engine compartment, leave this until last in case oil is picked up on the hands or gloves. Use vehicle search mirrors where issued. At the completion of the search, thank the driver and complete the search register, including full details of the vehicle.

General guidance.

Searching: people

Existing contingency plans to search people should be considered in the event of a raised threat and after:

- confirmation from intelligence agencies of an increased threat to crowded places
- consultation with centres to agree implementation operationally
- consultation with the communication director to agree public messaging and media management; and
- understanding that this would be a short-term measure in at a time of increased threat.

This measure should only be in operation while there is a still an ongoing threat. The method of search (i.e. bags, wands, etc.) should be determined by the nature of threat posed. If the decision to introduce searching of the public is implemented then:

- always be polite and explain what will happen and why the search is being carried out
- individuals carrying hand baggage should be asked to open them to reveal the contents; and
- personal body searching must not take place, bags and emptying of pockets only.

The security officer must always remember that they are not a policeman / policewoman and have no right of search without consent. If consent is not given then entry is to be refused. Staff should be trained and clear on what action is required should a suspicious item be found.

Appendix A
Bomb threat checklist

This checklist is designed to help your staff deal with a telephoned bomb threat effectively and to help you record the necessary information. Display it so that staff can see instantly.

Actions to be taken on receipt of a bomb threat

Record the EXACT wording of the threat. Ask the following questions:

- Where is the bomb right now?
- When is it going to explode?
- What does it look like?
- What will cause it to explode?
- Did you place the bomb?
- Why?
- What is your name?
- What is your address?
- What is your telephone number?

About the caller	What gender are they?
	How old do they sound?
	What is their nationality?
Language	Are they well spoken?
	Are they irrational?
	Are they being offensive?
	Is their voice taped or not?
Caller's voice	Are they calm or angry?
	Have they laughed?
	Is their voice disguised?
	Do they have an accent?
Background sounds	Are there any street noises?
	Can you hear any p.a systems?
	Are there any office noises?
	Can you hear any traffic?
Anything else noticed	What was the time of the call?
	What number did you receive the call from?

Now dial 999 without delay.

TERRORISM
IF YOU SUSPECT IT, REPORT IT
Confidential Anti Terrorist Hotline 0800 789 321 or if its happening now dial 999.

Bomb threat checklist.

Additional Information

Local advice
Your Counter Terrorism Security Advisor can be contacted via:
https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities

Additionally, the Revo Security and Safer Shopping Committee can provide further advice and guidance if required.

Guidance and action
A well briefed and well-rehearsed crisis management team should be appointed to address unforeseen incidents. Additionally, all staff should be trained to report anything suspicious as soon as possible.

Action Counters Terrorism
With the terror threat becoming increasingly complex and varied, police are calling on communities to act on their instincts to help prevent atrocities taking place in the UK and overseas.
https://www.gov.uk/government/news/action-counters-terrorism

ACT Awareness
ACT Awareness eLearning will provide nationally accredited corporate CT guidance to help industry better understand, and mitigate against, current terrorist methodology. Follow the link to the ACT Awareness e-learning programme
https://www.gov.uk/government/news/act-awareness-elearning

References.

CPNI Toolkits
The NaCTSO website
The Security Service website
The Centre for the Protection of National Infrastructure (CPNI) website

Revo Guidance Note 110: Managing Security in Retail Property
Revo Guidance Note 107: Insider Threat
Revo Guidance for General Managers: integrated safety management and major incidents in retail places
National Counter Terrorism Security Office (NaCTSO) Counter Terrorism Protective Security Advice for Crowded Places

Revo

Revo is the retail property community. We are the definitive go-to hub for the retail property and placemaking community. We represent and advance our members' interests, set standards and bring people together to collaborate and create tangible changes in our market.

Revo
13-15 Carteret Street Westminster
London
SW1H 9DJ
020 7227 4480
davinder@revocommunity.org
revocommunity.org