Counter Terrorism Awareness

Delegate workbook

skills for security
setting standards, raising skills

Counter Terrorism Awareness

The private security industry is now recognised as a critical business sector in its own right and makes a key contribution to the UK economy and to the security and safety of the nation.

It is therefore imperative that Skills for Security as the Skills and Standards Setting Body ensures that high quality training and development opportunities are available, to provide a highly skilled and professional workforce.

To further enhance training provision, we have accredited programmes that have been developed by other organisations that have met our quality standards.

It is extremely important that security personnel are prepared for a terrorist threat and we are pleased to accredit the terrorist Threat Awareness Course from Rutherford Training, as this course offers an understanding of how to deal with a terrorist attack and preventive measures to ensure safety.

Bob Doyle
Director of Commercial Services

skills for security
setting standards, raising skills

Delegate workbook

PURPOSE

This booklet is designed to accompany the course and consists of 4 main modules, which are:

1 **Terrorism module notes**

2 **IED module notes**

3 **AOP module notes**

4 **Post incident module notes**

1 Terrorism module notes

What is terrorism?

Terrorism is a term used to describe violence or other harmful acts committed (or threatened) against civilians by groups or persons for political or other ideological goals. Most definitions of terrorism include only those acts which are intended to create fear or 'terror', are perpetrated for an ideological goal (as opposed to a lone attack), and deliberately target non-combatants.

As a form of unconventional warfare, terrorism is sometimes used when attempting to force political change by: convincing a government or population to agree to demands to avoid future harm or fear of harm, destabilisation of an existing government, motivating a disgruntled population to join an uprising, escalating a conflict in the hopes of disrupting the status quo, expressing a grievance, or drawing attention to a cause.

Terrorism has been used by a broad array of political organisations in furthering their objectives; both right-wing and left-wing political parties, nationalistic, and religious groups, revolutionaries and ruling governments. The presence of non-state actors in widespread armed conflict has created controversy regarding the application of the laws of war.

In November 2004, a UN panel described terrorism as any act: intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organisation to do or abstain from doing any act.

Psychological impact and fear

An attack is carried out in such a way as to maximise the severity and length of the psychological impact. Each act of terrorism is a 'performance', a product of internal logic, devised to have an impact on many large audiences.

Terrorists also attack national symbols to show their power and to shake the foundation of the country or society they are opposed to. This may negatively affect a government's legitimacy, while increasing the legitimacy of the given terrorist organisation and/or ideology behind a terrorist act.

Perpetrated for a political goal

Something all terrorist attacks have in common is their perpetration for a political purpose. Terrorism is a political tactic, not unlike letter writing or protesting, that is used by activists when they believe no other means will affect the kind of change they desire.

The change is desired so badly that failure is seen as a worse outcome than the deaths of civilians. This is often where the interrelationship between terrorism and religion occurs.

When a political struggle is integrated into the framework of a religious or 'cosmic' struggle, such as over the control of an ancestral homeland or holy site such as Israel and Jerusalem, failing in the political goal (nationalism) becomes

The Threat of Terrorism
MODULE AIM
To understand the threat of terrorism
MODULE OBJECTIVES
Identify the cycle of a terrorist attack
Outline safety measures to be implemented

equated with spiritual failure, which, for the highly committed, is worse than their own death or the deaths of innocent civilians.

Deliberate targeting of non-combatants

It is commonly held that the distinctive nature of terrorism lies in its intentional and specific selection of civilians as direct targets. Much of the time, the victims of terrorism are targeted not because they are threats, but because they are specific 'symbols, tools, animals or corrupt beings' that tie into a specific view of the world that the terrorists possess.

Their suffering accomplishes the terrorists' goals of instilling fear, getting a message out to an audience, or otherwise accomplishing their political end.

Unlawfulness or illegitimacy

Some official (notably government) definitions of terrorism add a criterion of illegitimacy or unlawfulness to distinguish between actions authorised by a 'legitimate' government (and thus 'lawful') and those of other actors, including individuals and small groups.

Using this criterion, actions that would otherwise qualify as terrorism would not be considered terrorism if they were government sanctioned. For example, firebombing a city, which is designed to affect civilian support for a cause, would not be considered terrorism if it were authorised by a 'legitimate' government.

This criterion is inherently problematic and is not universally accepted, because: it denies the existence of state terrorism; the same act may or may not be classed as terrorism depending on whether its sponsorship is traced to a 'legitimate' government; 'legitimacy' and 'lawfulness' are subjective, depending on the perspective of one government or another; and it diverges from the historically accepted meaning and origin of the term. For these reasons this criterion is not universally accepted. Most dictionary definitions of the term do not include this criterion.

The difference between the words 'terrorist' or 'terrorism' and the terms above can be summed up by the aphorism, 'One man's terrorist is another man's freedom fighter.' This is exemplified when a group that uses irregular military methods is an ally of a State against a mutual enemy, but later falls out with the State and starts to use the same methods against its former ally.

During World War II the Malayan People's Anti-Japanese Army was allied with the British, but during the Malayan Emergency, members of its successor, the Malayan Races' Liberation Army, were branded terrorists by the British.

More recently, Ronald Reagan and others in the American administration frequently called the Afghan Mujahideen freedom fighters during their war against the Soviet Union, yet twenty years later when a new generation of Afghan men are fighting against what they perceive to be a regime installed by foreign powers, their attacks are labelled terrorism by George W. Bush.

Groups accused of terrorism usually prefer terms that reflect legitimate military or ideological action. Leading terrorism researcher Professor Martin Rudner, director of the Canadian Centre of Intelligence and Security Studies at Ottawa's Carleton University, defines 'terrorist acts' as attacks against civilians for political or other ideological goals, and goes on to say:

'There is the famous statement: 'One man's terrorist is another man's freedom fighter.' But that is grossly misleading. It assesses the validity of the cause when terrorism is an act. One can have a perfectly beautiful cause and yet if one commits terrorist acts, it is terrorism regardless.'

Some groups, when involved in a 'liberation' struggle, have been called terrorist by the Western governments or media. Later, these same persons, as leaders of the liberated nations, are called statesmen by similar organisations. Two examples are Nobel Peace Prize laureates Menachem Begin and Nelson Mandela.

Sometimes states that are close allies, for reasons of history, culture and politics, can disagree over whether members of a certain organisation are terrorists.

For example for many years some branches of the United States government refused to label members of the Irish Republican Army (IRA) as terrorists, while it was using methods against one of the United States' closest allies (Britain), that Britain branded as terrorist attacks. This was highlighted by the case, Quinn v. Robinson.

Many times the term 'terrorism' and 'extremism' are interchangeably used. However, there is a significant difference between the two. Terrorism is essentially a threat or an act of physical violence, whereas extremism involves using non-physical instruments to mobilise minds to achieve its political or ideological ends.

For instance, Al Qaeda is involved in terrorism. The Iranian revolution of 1979 is a case of extremism. A global research report, An Inclusive World (2007), asserts that extremism poses a more serious threat than terrorism in the decades to come.

Types of terrorism		
In the spring of 1975, Law Enforcement Assistant Administration in the United States formed the National Advisory Committee on Criminal Justice Standards and Goals. The Task Force classified terrorism into six categories.		
1	**Civil disorders**	A form of collective violence interfering with the peace, security, and normal functioning of the community
2	**Political terrorism**	Violent criminal behaviour designed primarily to generate fear in the community, or substantial segment of it, for political purposes.
3	**Non-political terrorism**	Terrorism that is not aimed at political purposes but which exhibits 'conscious design to create and maintain high degree of fear for coercive purposes, but the end is individual or collective gain rather than the achievement of a political objective.'
4	**Quasi-terrorism**	The activities incidental to the commission of crimes of violence that are similar in form and method to genuine terrorism but which nevertheless lack its essential ingredient. It is not the main purpose of the quasi-terrorists to induce terror in the immediate victim as in the case of genuine terrorism, but the quasi-terrorist uses the modalities and techniques of the genuine terrorist and produces similar consequences and reaction. For example, the fleeing felon who takes hostages is a quasi-terrorist, whose methods are similar to those of the genuine terrorist but whose purposes are quite different.
5	**Limited political terrorism**	Genuine political terrorism is characterised by a revolutionary approach; limited political terrorism refers to 'acts of terrorism' which are committed for ideological or political motives but which are not part of a concerted campaign to capture control of the State
6	**Official or State terrorism**	**Official or State terrorism** Referring to nations whose rule is based upon fear and oppression that reach similar to terrorism or such proportions'
7	**Religious terrorism**	**Religious terrorism** Violent terrorism that is committed in the name of a religion, usually by religious extremists. Some examples include the suicide bombings committed by Al-Qaeda, Hamas, and Hezbollah

For these and other reasons, media outlets wishing to preserve a reputation for impartiality are extremely careful in their use of the term.

Many of the most deadly operations in recent time, such as 9/11, the London Underground bombing, and the 2002 Bali bombing were planned and carried out by a close clique, comprised of close friends, family members and other strong social networks. These groups benefited from the free flow of information, and were able overcome the obstacles they encountered where others failed due to lack of information and communication.

Over the years, many people have attempted to come up with a terrorist profile to attempt to explain these individuals' actions through their psychology and social circumstances. Others, like Roderick Hindery, have sought to discern profiles in the propaganda tactics used by terrorists.

Tactics

Terrorist attacks are often targeted to maximise fear and publicity. They usually use explosives or poison, but there is also concern about terrorist attacks using weapons of mass destruction. Terrorist organisations usually methodically plan attacks in advance, and may train participants, plant 'undercover' agents, and raise money from supporters or through organised crime. Communication may occur through modern telecommunications, or through old-fashioned methods such as couriers.

History of Terrorism within the UK

5th November 1605: The Gunpowder- Plot Guy Fawkes attempt to blow up King James I and Parliament

21st June 1887: Jubilee Plot -Fenian agent attempts to blow up Westminster Abbey & Queen Victoria

19th September 1972: Israeli Embassy bomb-Black September group sends a letter bomb that kills a diplomat

21st November 1974: Birmingham Pub Bombings-IRA bombs kill 21 and injures another 182

30th April 1980: Iranian Embassy Siege-Six terrorists seize the building for six days until an SAS rescue mission

21st December 1988: Lockerbie Bomb-Pan Am flight 103 is destroyed by a suitcase bomb killing 270.

24th April 1993: Bishopsgate Bomb-A huge IRA truck bomb explodes in the Bishops gate area of London, killing 2 people and causes £350m in damage

15th June 1996: Manchester Bomb-1500kg truck bomb explodes destroying a shopping centre and injuring 206 people

15th August 1998: Omagh Bomb-29 people killed & another 220 injured in a Real IRA car bomb attack

3rd August 2001: Ealing Car Bomb-A car bomb explodes outside a busy pub injuring 7 people and causing massive damage

7th July 2005: London suicide bombings-Four separate suicide bombers detonate their devices on public transport killing 56 people and injuring 700

30th June 2007: Glasgow Airport-Two suspected suicide bombers drive a burning vehicle filled with Gas canisters into the main terminal at Glasgow International Airport.

Response to terrorism

Responses to terrorism are broad in scope. They can include re-alignments of the political spectrum and reassessments of fundamental values. The term counter-terrorism has a narrower connotation, implying that it is directed at terrorist actors.

Specific types of responses include:

- Targeted laws, criminal procedures, deportations, and enhanced police powers
- Target hardening, such as locking doors or adding traffic barriers
- Pre-emptive or reactive military action
- Increased intelligence and surveillance activities
- Pre-emptive humanitarian activities
- More permissive interrogation and detention policies
- Official acceptance of torture as a valid tool

Anti-terror organisations

Due to the ever present threat of terrorism in the UK there are certain key agencies, apart from the police, that play an important part in the prevention, detection and investigation of potential terrorist activity. All of these agencies work closely together to raise awareness and prevention as well as putting into place response and contingency plans in the event of an attack, either attempted or successful.

NaCTSO

The National Counter Terrorism Security Office is a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). They are directly accountable to the Association of Chief Police Officers (ACPO).

NaCTSO works closely with the Security Service to reduce the potential impact of terrorism within the UK. Their aims are to raise awareness of the terrorist threat and the measures that can be taken to offset and reduce these threats, deliver protective security advice and contribute to the development of the national counter terrorism policy. They provide guidance in relation to business continuity and the protection of crowded places and reducing opportunities for terrorism through the design of the working environment.

NaCTSO also is responsible for training and providing specialist police advisers known as Counter Terrorism Security Advisers (CTSAs), whose role it is to provide help, advice and guidance on all aspects of counter terrorism protective security.

If you require further advice on protective security measures, contact your local police crime reduction officer who may, if required, refer you to your CTSA.

Remember that if you wish to report any suspicious activity you should contact either your local police force or the Anti-Terrorist Hotline on 0800 789 321.

CPNI

CPNI
Centre for the Protection of National Infrastructure

Centre for the Protection of the National Infrastructure is the government organisation which provides security advice to businesses and organisations involved with the running, operating and supporting of the national infrastructure.

The CPNI provides expert advice to the critical national infrastructure on physical, personnel and information security, to protect against terrorism and other threats.

The CPNI was formed by the merger of the National Infrastructure Security Coordination Centre (NISCC) and a part of MI5 (the UK's Security Service) and the National Security Advice Centre (NSAC).

NISCC used to provide advice and information on computer network defence and other information assurance issues. NSAC provided advice on physical security and personnel security issues.

CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organisations which make up the national infrastructure. Through the delivery of this advice they aim to protect national security, by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

They are an interdepartmental organisation, with resources from a number of government departments and agencies. These include MI5, CESG (Communications Electronics Security Group) – the UK's National Technical Authority for Information Assurance and other Government departments responsible for national infrastructure sectors.

They are accountable directly to the Director General of the Security Service (MI5).

Project Griffin

Project Griffin was formally introduced in April 2004 as a Pan London project uniting the Police (Metropolitan and City of London), local authorities, private sector security industry, London Fire Brigade, London Ambulance Service and other agencies to coordinate effort by working together to deter, disrupt and support pro-active operations regarding terrorist/extremist activity within London.

Since its inauguration Project Griffin has been identified nationally as good practice and is now well established in a number of Police Forces around the country, encouraging members of the community to work in partnership with the police to deter and detect terrorist activity and crime. This will be achieved by working with the community to:

- Raise awareness of current terrorist and crime issues
- Share and gather intelligence and information
- Build and maintain effective working relationships
- Seek solutions to defeating terrorism and crime
- Maintain trust and confidence in the Police and other authorities
- Empower people to report suspicious activity and behaviour.

The main strand of Project Griffin is very much about the police sharing information with key trusted partners in the community, by providing input through an 'Awareness Day'.

Awareness Days

The Awareness Day is delivered in a structured way, covering topics such as the current threat level, hostile reconnaissance, recognising the components of an explosive device and person/vehicle borne devices helping to galvanise and motivate participants to want to work with the police.

Who is eligible to attend?

Project Griffin is aimed at people involved with the safety and security of a building, business or arena, enabling them to recognise and report suspicious activity and behaviour to the police. The Awareness Day helps people identify their own local procedures and processes for dealing with emergency incidents.

Initially we engage and empower people to build relationships and encourage reporting. Secondly we explain the concepts of providing information by means of a regular 'Bridge Call' and agreeing protocols to assist police resources (in times of extremis). Cordons and high visibility patrolling are all tried and tested initiatives which also help to maintain participants involvement, making them feel like members of the extended police family.

Emergency Deployment

Where local protocols are in place, the police may request participating organisations to make available Project Griffin trained personnel.

Where Project Griffin personnel are deployed alongside the Police they will work under the direction of the police utilising civilian powers.

The Police may also request participating companies and organisations to increase visibility around their own premises and request that Project Griffin personnel undertake and increase exterior patrols of their buildings to increase high visibility patrolling in the local area.

Contact details
for further information please contact your local police force or:
Ian Mansfield
Counter Terrorism Security Advisor
Police Headquarters
37 Wood Street
London, EC2P 2NQ

Email:
ian.mansfield@city-of-london.police.uk
Telephone: 020 7601 2863

Martin McGuiness

In a historic moment for Northern Ireland, Sinn Féin's Gerry Adams and Martin McGuinness last night backed the police manhunt and denounced the attackers. McGuinness, the deputy first minister, said: "I was a member of the IRA, but that war is over now. The people responsible for last night's incident are clearly signalling that they want to resume or restart that war. Well, I deny their right to do that."

March 2009

Project Argus – Protecting Against Terrorist Attacks

Project ARGUS (Area Reinforcement Gained Using Scenarios) is a National Counter Terrorism Security Office (NaCTSO) initiative, which explores ways to aid businesses in preventing, handling and recovering from a terrorist attack.

The terrorist attacks in London during July 2005 dramatically highlighted the need for businesses of all sizes, to plan how they deal with the disruption caused by a major crisis, emergency or incident. Recent events in London and at Glasgow airport, along with a number of convictions for terrorism related offences, further demonstrate that we must not become complacent.

The aim of Project ARGUS, is to increase awareness of counter terrorism issues and help make us more resilient as a community.

Project ARGUS takes delegates through a multi-media simulation of a series of terrorist attacks, occuring in a shopping centre, which provides them with a unique opportunity to learn and share knowledge and experiences. The scenario explores peoples options and possible reactions following an attack and considers their initial priorities, before tackling issues of business continuity and, finally, prevention of future attacks. Delegates also receive valuable information and advice from the Corporation of London, the London Ambulance Service and the London Fire Brigade who form an expert panel.

The project highlights the importance of businesses being prepared by having the necessary plans in place to help safeguard staff, customers and company assets. It also emphasises the need to practice those plans regularly. Project ARGUS is a key part of the City of London polices' overall aim to reduce the risk from terrorism, so that people can go about their daily lives and business freely, and with confidence.

The Counter Terrorism Section facilitates the Project ARGUS sessions and the feedback received has been extremely positive. Project ARGUS is helping to protect people, businesses and also the wider community by raising awareness and offering practical advice and support. It encourages businesses in the local area to work together and in partnership with the emergency services and the Corporation of London.

The Security Service

The Security Service, or MI5 (Military Intelligence, Section 5), is the UK's counter-intelligence and security agency. They work closely with other intelligence organisations such as, Secret Intelligence Service, Government Communications Headquarters (GCHQ) and the Defence Intelligence Staff. All of these agencies come under the direction of the Joint Intelligence Committee.

Its remit includes the protection of British democratic and economic interests, fighting serious crime, militant separatism, terrorism and espionage within the UK.

The Muslim Council of Britain

"All of us have an important stake in ensuring that our country is properly safeguarded from those who want to launch indiscriminate attacks. It is crucial that all of us, Muslim and non-Muslim, give the necessary help and support to those charged with responsibility of maintaining our security"

Dr Mohammed Abdul Bari

Secretary General of The Muslim Council of Britain

March 2009

2 IED module notes

Improvised Explosive Devices

Improvised Explosive Devices, or as they are more commonly known IEDs, are a common but powerfully effective weapon in the modern day terrorist's arsenal.

In today's complex and difficult society the threat of a terrorist attack is a very real possibility. With the recent rise in global terrorism most high profile targets such as governmental, police or military locations are well prepared and secured so the terrorist has had to look elsewhere for viable targets. Due to this fact so called 'soft' targets, which previously might not have chosen, have become the focus for attacks due to their ease of access, lack of awareness and reduced security precautions.

Transport hubs such as train stations and airports or social venues such as bars and night clubs have been targeted on numerous occasions both recently and historically by terror organisations or individuals. Due to this the need for increased vigilance and awareness of the threat is becoming ever more important for all of us.

IEDs have been around since the invention of old fashioned gunpowder and have been used, successfully, for centuries. From simple fireworks and home made fire crackers right through to car bombs, or as in Iraq and Afghanistan where they are often referred to as roadside bombs, IEDs are recognised the world over.

Due to the dangerous nature of explosives, most governments around the world restrict their sale, supply and distribution, thereby making it difficult for criminals or terrorists to obtain military or commercial grade high powered explosives.

To this end terrorists have to resort to either stealing their explosives or, as is more common, manufacturing their own supply of explosive material from readily accessible materials. Over the years knowledge and understanding about the production of explosive materials has become quite advanced amongst terrorists and they are capable of producing extremely high powered explosives. With the introduction of the internet, a terrorists capability to share their expertise in production, and indeed construction techniques, has dramatically increased, along with the threat we face.

The history of improvised explosive devices

As mentioned, IEDs have been used, for centuries. However, over the last 80 years their use has seen a dramatic surge, partly due to our increased understanding of explosives and their increasing power and reliability.

World War II

The Second World War saw the IED become a viable tool in the saboteur's arsenal when underground, or rebel forces used them to great effect against the occupying troops of the Axis forces. In Russia during the so called Rail War of 1943–1944 Belarusian forces used large numbers of simply constructed home made IEDs in large scale co-ordinated attacks on German supply and troop

IEDs

MODULE AIM

To exlore IEDs

MODULE OBJECTIVES

Illustrate what an IED is

Explain the IED key components

Discribe the different IED device types

Household materials used to make explosives

- Nail polish remover – *acetone*
- Aspirin – *acetylsalicylic acid*
- Rubbing alcohol or spirits – *alcohol*
- Salt substitutes – *potassium chloride*
- Liquid plant feed – *potassium chloride*
- Oven degreaser – *ammonia*
- Window cleaner – *ammonium hydroxide*
- Garden fertiliser – *ammonium nitrate*
- Car batteries – *sulphuric acid*
- Household cleaners – *nitric acid*
- Hair dyes – *hydrogen peroxide*
- Disinfectants – *potassium chlorate*
- Pesticides – *potassium chlorate*
- Baking soda – *sodium bicarbonate*
- Fridge deodorisers – *sodium bicarbonate*
- Antacids – *sodium bicarbonate*
- Wax/Vaseline to solidify the explosive
- Bleach
- Coffee filters
- Sugar
- Cotton wool

trains to great effect. These attacks limited the German advance into Russia and severely damaged supply lines but more importantly undermined the morale of the German forces.

The British Special Operations Executive (SOE) also used IEDs to great effect in combating German and Italian forces throughout the war. Including the legendary tale of putting explosives inside rats and nice and then placing these IEDs in ammunition stores or by the roadsides where they were often overlooked until they detonated.

Northern Ireland

The IRA and other paramilitary organisations involved in the troubles in Northern Ireland have made extensive use of IEDs over the years. The use of the petrol bomb, or Molotov cocktail, being the simplest form of an IED right through to highly sophisticated remotely detonated devices these organisations gained vast experience in the use and construction of IEDs.

Due to the intervention of the armed forces large numbers of the terror groups IEDs were disarmed and they then had to seek ever more advanced and sophisticated means of construction and concealment for the devices.

Vietnam War

Throughout the Vietnam War the Viet-Cong forces were constantly short of supplies, munitions and military equipment. So they often had to make do with IEDs to combat the heavily equipped US forces and they very quickly became proficient in their use and construction.

Often they would reuse the explosive material from unexploded US weapons that had been fired or dropped on them. The effectiveness of this tactic was borne out by official US figures which placed US casualty figures at around 28% linked to mines and booby traps, the majority of which consisted of IEDs.

They specialised in hiding IEDs in bamboo huts, or under piles of bamboo, this was due to the fact that the US forces would often burn huts to prevent their use by Viet-Cong forces. When the huts or bamboo was burnt the IED would detonate and the bamboo would then be turned into lethal flying shrapnel.

Afghanistan

Throughout the Russian incursion into Afghanistan in the 1980s the Mujahideen forces used large numbers of IEDs to target their personnel, equipment and bases. The Mujahideen were initially supplied with outdated military equipment from the west and Arabic states to combat the threat of communist forces.

However they found that the anti tank mines they had weren't really up to the job, so often they would use

the material from several mines to home make a larger more powerful IED. These they placed in cooking oil cans or oil drums to increase their power further, but these were easily spotted or detected by metal detectors.

Once they realised this the Mujahideen began placing them into plastic boxes or containers which made them much more effective weapons, they might have been less powerful but were rarely detected in time.

Since 2001 the Taliban has employed similar tactics and IEDs to launch attacks on Coalition forces within the country, again with deadly results.

Animal rights

Often IEDs are considered the tool of terror organisations but anti-vivisectionists, anti-fur groups and animal rights groups such as ARM (Animal Rights Militia) have used IEDs for their own campaign of terror within the UK. In 1982 several letter bombs were sent to then Prime Minister Margaret Thatcher at 10 Downing Street, signed by the Animal Rights Militia. This campaign resulted in the injury to one individual, but its principal effect was to disturb the operation of the government.

Throughout the 1980s anti-fur groups waged a campaign to prevent the sale of real fur products through the UK, this campaign included fire bombing and sending letter bombs to stores selling and carrying fur products as well as targeting the suppliers and distributors of the furs. They also made threats and carried out several attempted attacks on high profile fashion designers and celebrities who appeared to endorse or support the industry.

Animal rights groups and anti-vivisectionists have also led a concentrated and extended campaign against laboratories and scientific testing organisations such as Huntingdon Life Sciences. There campaigns have been largely peaceful but there have been incidents involving detonating firebombs at the homes and offices of people and organisations who work for or with the testing facilities.

Iraq

Iraqi rebels and insurgents have been highly successful at implementing the use of IEDs to combat the coalition forces within the country. According to the organisation iCasualties.org 38 percent of US casualties are as a result of IEDs.

Due to the nature of the situation in Iraq there is a multitude of materials available to these terror groups and they have proved extremely resourceful at building and concealing their IEDs. There have been discoveries of IEDs being concealed by the roadside in everything from soft drinks cans and bottles to animal carcasses. These devices have proved deadly due to the ready access to high explosive materials in the country and the expert training that many of the builders received either from under the previous Iraqi regime or from training received abroad.

IEDs are not only being employed against military and police targets but have also been used frequently against the innocent civilian population at locations such as markets and Mosque's.

The UK

IEDs are an ever present threat and, as discussed, are often constructed from home made materials; in fact simple common garden fertiliser is a common ingredient in manufacturing many explosive materials.

This was highlighted in detail on the 30th March 2004 when the Metropolitan police raided several locations as a result of *Operation Crevice*. This resulted in the arrest of at least 6 people and the seizure of 600 kg of ammonium nitrate fertiliser, which was destined to make IEDs.

The chemicals were found in a storage space in Hanwell in West London, and the majority of the suspects were arrested near Crawley where police also discovered a tin of aluminium powder, another principal ingredient for bomb making.

During the police investigation it was discovered that the suspects had planned to construct and detonate IEDs at locations such as Bluewater shopping centre, Ministry of Sound nightclub and synagogues around London.

The power and effectiveness of IEDs was highlighted with devastating effect on 7th July 2005 in London when four suicide bombers detonated their IEDs with lethal consequences. These coordinated attacks resulted in the deaths of 56 people and injuring another 700 not to mention the psychological and economic impact they had on the country as a whole.

All four devices were manufactured at home and concealed in rucksacks. Police also found a further 16 bombs in one of the suspects vehicles, including several nail bombs.

And only recently we received yet another warning of the danger of IEDs from the attack on Glasgow Airport, where a vehicle packed with explosive gas canisters was set alight and driven into the entrance of the main terminal. This attack followed on from the discovery and disarming of a large car bomb that was discovered by a member of the public in London's Haymarket area, right outside a busy nightclub.

What is an IED?

An IED is basically a bomb which has been built using whatever materials and equipment the terrorist bomb maker had at their disposal or access to, it usually consists of 5 key components.

As mentioned IEDs come in all sorts of shapes and sizes but the main advantages over the use of a conventional weapon, such as a gun or knife, is that they are relatively cheap to produce. Since they can be made from commonly and easily accessible materials such as household items, they tend to arouse very little suspicion and can be put together quite quickly without the need to be hidden for very long. Also as they are improvised they can be tailored or adapted easily to suit the selected target type and location.

Components of an IED

1. Switch – a device to prime the weapon's circuit
2. Main explosive charge – home made or military issue material
3. Power source – such as a battery
4. Initiator – or a detonator, a small charge to ignite the main explosive charge
5. Container – numerous possibilities such as a tin can or a plastic lunch box

The 5 key IED device types:

Over the years there have been many kind of devices that have been used by different organisations ranging from the fire bombs employed by anti fur campaigners in the 80s, nail bombs such as the Admiral Duncan pub bombing, suicide bombs as in London on July the 7th 2005 right up to the recent wave of letter bombs directed towards the DVLA and Police stations.

It's worth taking some time to understand the different kinds of devices and their construction and the threat that they pose. All IEDs fall into one of 5 key activation or detonation types.

The choice of method of activation or type depends upon the terrorists goals and aims as well as the intended target.

As well as having a choice of the way in which the device can be activated the terrorist also has to consider how the device is going to be delivered to its chosen target. This will include looking at how the device is going to be concealed; these methods of concealment and delivery tend to fall into one of three categories:

1. Package type
   - These are the most common type of device that has been employed in the past, and is what we would perceive as the 'suspect package'
   - A suitcase, bag or box left at or near the target
   - Letter or parcel bomb sent to a target

2. Vehicle borne IEDs (VBIEDs)
   - The preferred method of delivery for large devices
   - Sometimes used to smash through external security precautions
   - Commonly a car or truck bomb
   - Any vehicle can be used depending upon the target

3. Suicide bomb
   - Highly difficult to detect
   - Used principally to target people not locations
   - Any device delivered to the target by an individual who intends to die whilst detonating the device

5 types of IED

1. Time activated – set to detonate at a particular moment
2. Command – detonated at a specific time, by mobile phone or radio
3. Victim Operated – set off by the intended victim, i.e. when the sensor in the device detects motion or a pressure activated device
4. Projected – throw or fired at the target
5. Suicide – carried by the human body or in the vehicle driven by the bomber

Person borne devices

IEDs that are delivered to the target by hand are usually carried in containers such as rucksacks, bags or briefcases, which are chosen to blend in easily with the target surroundings.

Due to the fact that they have to be easily portable, such devices are unlikely to weigh more than 25kg, although even an ordinary-sized briefcase can contain about 12kg of explosive charge. A 25kg suitcase bomb could destroy a house or cause serious structural damage to larger buildings.

Pipe Bomb

A pipe bomb is a usually a short piece of steel piping that contains an explosive mixture and is sealed at both ends with screwed or welded caps. A fuse is inserted into one end of the pipe with a lead running out through a hole of one of the

caps, this is often attached to a timer and battery or it could be a basic wick as is used for a firework.

Most of these components are very easily accessible and the devices are relatively simple to manufacture. Despite the fact that the explosive material tends to be quite basic and low powered, the way they are constructed produces a large explosion and the fragmentation of the pipe creates lethal shrapnel.

Nail bomb

A nail bomb is just an extension of any other type of explosive device. They are usually constructed by placing quantities of household nails and screws inside the bomb, and quite frequently packing and surrounding the device with even more nails and screws. The idea behind a nail bomb is that when the device is detonated the nails will increase the amount of shrapnel flying through the vicinity of the detonation, and multiply the number and severity of the injuries sustained by the victims.

The most well known incident involving the use of a nail bomb was David Copeland's attack on the Admiral Duncan pub in London's Soho on the 30th April 1999.

Other materials have been attached to devices in the past, such as scrap metal or ball bearings but these are generally all referred to as nail bombs. Terrorists have often coated the nails or shrapnel in poison, or even human excrement, to increase the potential lethality of the devices by causing poisoning or infection.

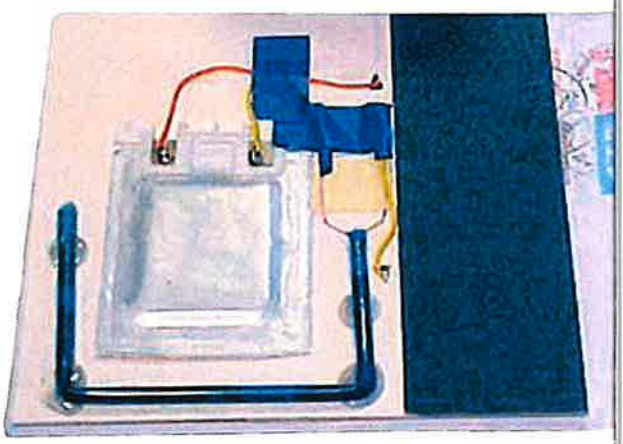
Letter bomb

A letter or mail bomb is an explosive device that is sent via the postal service, and designed with the intention to injure or kill the recipient when opened. They have been used by terrorists and activist groups in their campaigns

Mail bombs are usually set to explode immediately on opening, with the intention of seriously injuring or killing the recipient. Parcel bombs may have excessive postage, as the bombers usually do not want to send a suspect parcel over the counter, thereby not having to deal with postal staff. Letter bombs often feel rigid, or appear uneven or lopsided.

Package bombs may have an irregular shape, soft spots, or bulges. Oil or grease stains are also indicators and act as warning signs. A related threat is mail containing unidentified powders or chemicals. In some cases, these turn out to be harmless, sent as a joke or hoax threat.

Letter bombs have been used by numerous groups such as ARM (Animal Rights Militia) or by individuals such as the series of letter bombs in early 2007 that was directed at the DVLA (Driver and Vehicle Licensing Agency) and organisations that deal with processing congestion charging and speeding fines.



Incendiary (Fire) bomb

These are generally either hand-carried devices or postal devices and are often deployed against economic targets such as retail outlets and transportation. The usual intention is to cause economic damage and weaken public confidence rather than cause mass casualties.

When planning protective measures, remember that incendiaries are generally small, that they ignite rather than explode (often when the target premises are empty) and that there is usually more than one device. The attacker will regard the attack as a success even if they do no more than trigger the sprinkler system, which itself can damage stock or furnishings. Incendiary devices are fairly simple to make and do not require access to explosives.

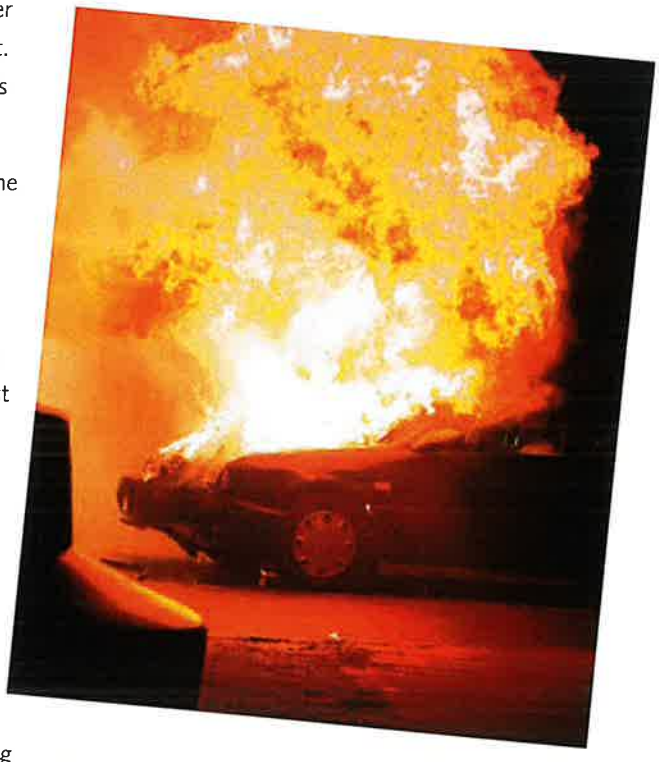
They may be used by disgruntled employees or customers in retaliatory attacks against companies and employers. They were also used by the anti-fur campaigners in the 1980s and recently by anti-globalisation activists at things such as the G8 summits around the world.

Vehicle borne improvised explosive devices (VBIEDs)

Car bomb

A car bomb is the most common form of VBIED that is used by modern day terrorists, it principally consists of an IED either built into or hidden within a car. The use of the car allows terrorists to use a larger payload than could be used in an IED hidden inside a bag or letter bomb. This increase in the payload has the added effect of providing a much bigger blast and a huge increase in the damage or casualties sustained in the attack.

This use of the car also enables the terrorist to transport the IED over greater distances and with more security than using public transport. The car also acts as a source for material as its bodywork and chassis provide a massive amount of shrapnel in the blast.



Car bombs have been used to target both people and buildings in the past. Also car bombs have been used as assignation tools, where an IED has been placed on or under a targets car and then detonates killing its intended victim.

In the past car borne IEDs were linked into the vehicles ignition, but this has fallen out of use, due partly to the advanced natures of most cars anti-theft systems.

As seen in the attack on Glasgow Airport car bombs are now being used by suicide bombers to ram the car, and the IED, into their target before detonation.

Motorbike bomb

As the type of IED varies so can the VBIED, motorbikes have been used in terror attacks in Iraq, Afghanistan and recently in Thailand. Motorbikes offer similar advantages to cars such as increased carrying capability and ease of movement of the device.

The explosives can quite easily be hidden under the seat, in the tank or fairing or even in panniers and bags on the machine.

Also due to the size and manoeuvrability they can gain access to areas that cars can not, also they have a lower profile compared to a car or lorry, and may arouse less suspicion. Furthermore they are cheaper and easier to obtain than a car or lorry.

On the 28th May 2007 an IED exploded in front of a busy market in the Saba Yoi area of Songkhla Province, South Thailand. The bomb, which exploded at around 4pm, was found to have been hidden in a motorcycle parked at the front of the market. The motorcycle was destroyed by the blast, and a nearby car damaged, as were dozens of stalls belonging to fruit and vegetable vendors.

Bicycle bomb

Bicycles or push bikes offer the terrorist similar advantages to using a motorbike but also have the added advantage of being able to enter pedestrian areas such as shopping centres and parks.

Since the explosives can be hidden within the actual frame of the bike or in panniers the can be extremely hard top identify.

Bicycle bombs have been used effectively by terrorist organisations the world over, from Sri Lanka, Pakistan, Afghanistan to Iraq. In fact the IRA used a bicycle bomb in 1939 in Coventry which killed 5 people.

Water borne bomb

In the past there have been attacks on targets using boats and ships to transport IEDs to their targets. This is of consideration to any building, location or facility that is either on or near a waterway such as a river, lake, canal or even the sea.

Since many major cities are built around a river these waterways can provide the terrorist with easy access to targets, indeed it is an ideal way to target infrastructure such as road or rail bridges as well as other vehicles using the waterway. Due to the nature of waterborne vessels they can carry an extremely large load of explosives.

The most famous incident involving water borne IEDs is the attack on the USS Cole this attack took place on the 12th October 2000 when the ship was attacked by a small boat carrying Al-Qaida suicide bombers. The ship was in the port of Aden in Yemen in the Persian Gulf. The attack resulted in the deaths of 17 sailors and another 39 injured.

Suicide bombers

A suicide bomber poses a totally different type of threat than any other kind of device mentioned earlier. Often the main aim of a suicide bomber is not just to commit suicide, but it is to kill, maim and injure as many people as they possibly can. They also hope to inspire fear and terror within the target community and get the people they are opposing to give in to their demands or goals.

A standard suicide bomber's explosive device tends to usually utilise only a small amount, roughly between 5 to 20 kilograms, of a high powered explosive

material, this is to ensure they cause the maximum amount of damage to the intended blast area. Frequently suicide bombers combine their explosives with other materials, often nails, screws, metal shards or ball bearings this is to increase the amount of injuries or fatalities they may cause.

Also the majority of suicide devices over the years have tended to utilise a manual detonation system, such as a hand held trigger or switch, that the terrorist activates. The combination of a relatively small device being carried on the person coupled to a simple trigger mechanism, creates a problem as it makes the devices very easy to conceal.

Another massive issue is that terror organisations never give a bomb threat warning for a suicide blast, unlike quite frequently when a device has been placed. A suicide bombing is simply designed to inflict harm, but more importantly to inspire terror, whereas a planted device is quite often more a demonstration of the terrorist's power and intent.

Since the main aim of most suicide bombings is to terrorise the community and general public, the bombers operations tend to focus upon targeting large public gatherings in areas such as: markets, shopping centres, city centres, nightclubs, restaurants, hotels, public transport and places of religious worship or significance.

Devices are carried in:
Vests – so called suicidevests
Aprons
Belts
Rucksacks
Satchels
Shoes
Underwear – such as a bra or boxer shorts
Packing boxes
Gym bagsBriefcases
Guitar cases
Computers
TV cameras
Birdcages
Watermelon

A suicide bombing is seen, by the terrorists, to have several key advantages over a planted device. A major one being that when a terrorist leaves an explosive devise at the designated target and escapes to safety prior to detonation, there is a possibility that the explosive device can be found and the area evacuated or the device made safe. Some other reasons are:

- The device is precisely delivered to the target
- The suicide bomber functions as a precision weapon, taking the explosive devise right to the target
- The terrorist is 'invisible' (stealth – masked) until the device is detonated
- Because the explosive device is guided by a human, it also has the ability to change locations at the last second in case the primary target is too difficult to reach, or a better target opportunity presents itself
- No planned egress is required
- The explosive charge simply has to be delivered to the target and detonated
- No one is left alive to interrogate
- Operational security within the terrorist group is better maintained
- No burden of wounded comrades exists
- The psychological fear and terror it inspires amongst the public

Chemical, biological or radiological attacks

Terrorists are always looking for a way to increase the effectiveness of their attacks, and over the last couple of decades there has been discussion of terrorists attempting to obtain ever more powerful weaponry. One of the avenues that they have attempted is to obtain nuclear, biological or chemical weapons.

The threat of a terrorist nuclear, biological or chemical attack has always been perceived as a remote possibility. There are numerous reasons for this, one being that these materials are extremely expensive and time consuming to produce and manufacture, not to mention that the equipment required is often heavily restricted and monitored. So attempting to produce any of these materials tends to arouse the suspicion and interest of the authorities.

Another principal reason is the difficulty in obtaining these materials from other sources as well as the complexity of using them effectively and safely. However, with the collapse of the former Eastern Bloc, and the increased financing and funding of terror groups, the fear has been that former military scientists and chemical weapons engineers might be tempted to sell their knowledge, experience and technical skills to terrorist organisations.

The problem with CBR attacks is that they have devastating consequences and the full effects of the attack might not be known for an extended period of time.

These differing types of devices have wide ranging and almost unlimited potential for death and destruction:

Nuclear devices

- Former Soviet suitcase bombs have allegedly disappeared and may be in terrorist hands
- Nuclear blast totally destroys the blast site
- Ongoing illnesses caused by exposure to radiation
- A dirty bomb is typically a device where radioactive materials are combined with conventional explosives designed to contaminate the area
- As well as large number of casualties from an initial blast, these devices have a longer-term threat to health

Nuclear devices:
Former Soviet suitcase bomb
Dirty bomb

Chemical devices

These devices are designed to poison or injure people by using chemical compounds or substances.

These materials may include ex-military chemical warfare agents or legal but harmful household and industrial chemicals.

Biological devices:
Anthrax
Ebola
Bubonic plague
Smallpox

Biological devices

These devices would be designed to use a biological bacteria or virus to cause death through illness and diseases.

Over the years numerous diseases have been considered to be turned into a weapon.

Chemical devices:
Botulinum – known as Botox commercially
Mustard gas
Nerve gas
Ricin
Saxitoxin

In the past 20 years there have been very few documented cases of a terrorist attack that has involved the use of a form of CBR material. The two most high profile incidents recorded are:

The Tokyo subway sarin attack

On the 20th March 1995 the Japanese religious group, Aum Shinrikyo, committed a coordinated attack on the Tokyo subway system. They simultaneously released 5 canisters containing Sarin on different lines running through the Tokyo subway.

The attack was committed at the height of the rush hour. Each of the terrorists had a plastic bag containing around one litre of liquid Sarin which had been wrapped in newspapers. This amount is huge when you consider that a single drop of Sarin the size of the pin head is enough to kill an adult.

Each terrorist carried their packets of Sarin and an umbrella with sharpened tips, at target stations, each terrorist dropped their package and pierced it several times with the sharpened tip of the umbrella before escaping.

The result of this attack was that 12 people lost their lives and another 50 people suffered severe injuries and required hospital treatment. However over 1000 people reported temporary breathing and vision problems, which shows how lucky the public was that the death toll wasn't higher.

US anthrax letter attacks

This series of attacks began on the 18th September 2001, only a week after the attacks on the World Trade Centre. A series of letters were sent to several targets throughout the US, the letters all contained Anthrax spores and were targeted at several American news and media offices as well as at two US Senators.

This series of attacks resulted in the deaths of five people and infected 17 others who required lengthy hospital treatment.

CBR attack response

Responding to an incident involving CBR material varies more than an incident involving a conventional or incendiary IED, but the major point is that the exact nature of the incident may not be immediately apparent.

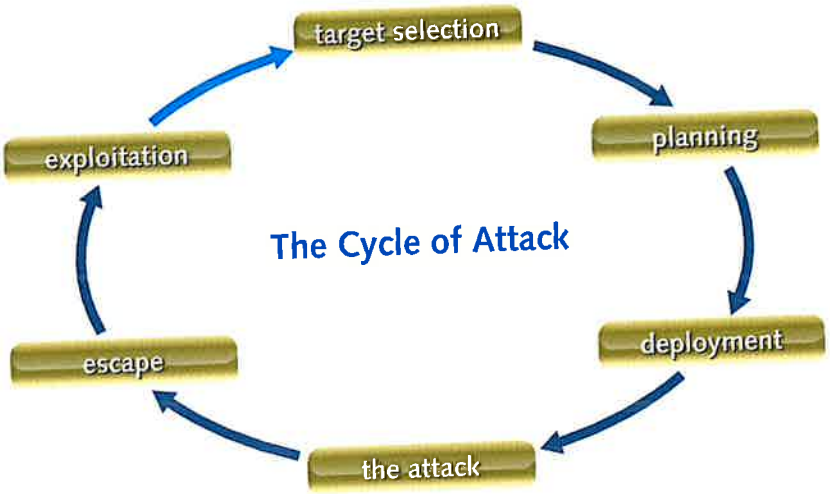
In the event of a suspected CBR attack certain steps should be taken to attempt to limit the potential impact of the attack.

For more information on nuclear, biological and chemical devices – their effects and symptoms, visit http://www.rtc-training.co.uk/IED-appendices.php

NBC attack response
To limit the impact of an attack
Switch off all ventilation systems that circulate the air
Air conditioning
Heating systems
Fans
Personal computers
Do not allow anyone, whether exposed or not, to leave evacuation areas before the emergency services as they may require
Decontamination
Medical advice
Assessments or treatment
If an incident occurs outside the building, close all doors and windows and switch off any systems that draw air into the building

The Cycle of Attack

Attacks designed to instill terror, not only among the surviving victims and those in the immediate vicinity of the violence, but among society in general, always appear to occur suddenly — to come "out of the blue." The actual event, however, is the culmination of the six-stage attack cycle:



During the target selection and planning stages, terrorists conduct pre-operational surveillance. In this stage, terrorists are no different from other criminals in preparing for an operation. The complexity and extent of the surveillance, however, vary with the scale of the operation and the end goal. A purse snatcher, for example, might size up the target for only a few seconds, while pre-operational surveillance for a terrorist attack could take several weeks.

The purpose of surveillance is to determine the target's patterns of behavior if it is an individual, or possible weaknesses and attack methods if the target is a building or facility. When the target is a person, perhaps targeted for assassination or kidnapping, terrorists will look for things such as the time the target leaves for work or what route is taken on certain days. They also will take note of what type of security, if any, the target uses. For fixed targets, the surveillance will be used to determine patterns and levels of security. For example, the plotters will look for times when fewer guards are present or when the guards are about to come on or off their shifts. In both cases, this information will be used to select the best time and location for the attack, and to determine what resources are needed to execute the attack.

Because part of pre-operational surveillance involves establishing patterns, terrorists will conduct their surveillance multiple times. The more they conduct surveillance, the greater the chances of being observed themselves. If they are observed, their entire plan can be compromised by alerting security personnel to the fact that something is being planned. Conversely, the terrorists could end up being surveilled themselves and can unwittingly lead intelligence and law enforcement agencies to other members of their cell.

Despite some impressions that Al-Qaeda is capable of conducting stealthy, clandestine surveillance, evidence recovered in Afghanistan during the US-

led invasion in October 2001 and other places suggest that most of the terrorist network's surveillance is sloppy and even amateurish.

Al-Qaeda training manuals, including the infamous "Military Studies in the Jihad against the Tyrants," and their online training magazines instruct operatives to perform surveillance, and even go so far as to discuss what type of information to gather. The texts, however, do not teach how to gather the information. This is the stage at which Al-Qaeda's operations often have found to be lacking.

The skills necessary to be a good surveillance operative are difficult to acquire, and take extensive training to develop. It is extremely difficult, for instance, to act naturally while performing an illegal act. Quite often, surveillance operatives will get the so-called "burn syndrome," the feeling that they have been detected even though they have not. This feeling can cause them to act abnormally, causing them to blow their cover. As a result, it is very easy for amateurs to make mistakes while conducting surveillance, such as being an obvious lurker, taking photos of objects or facilities that would not normally be photographed, and not having a realistic cover story when confronted or questioned.

In some cases, however, al Qaeda operatives have conducted extensive, detailed surveillance of their potential targets. In July 2004, the arrest in Pakistan of an individual identified by U.S. officials as Mohammad Naeem Noor Khan revealed a personal computer that contained detailed information about potential economic targets in the United States. The targets included the New York Stock Exchange and Citigroup headquarters in New York, the International Monetary Fund and World Bank buildings in Washington, D.C., and Prudential Financial headquarters in Newark, N.J. From the information on the computer, it appeared that the targets were under surveillance for an extended period.

Countersurveillance — the process of detecting and mitigating hostile surveillance — is an important aspect of counterterrorism and security operations. Good countersurveillance is proactive; it provides a means to prevent an attack from happening. Countersurveillance can be an individual or group effort, involving a dedicated countersurveillance team. Individuals can and should conduct their own countersurveillance by being aware of their surroundings and watching for individuals or vehicles that are out of place.

Countersurveillance is the proactive means of spotting terrorist and criminal surveillance during the target selection and planning stage — the time the operation is most vulnerable to interdiction. Law enforcement and intelligence agencies, corporations and individuals must understand the importance of countersurveillance — and be capable of recognizing hostile surveillance before the next phase of the attack cycle begins. Once the actual attack has begun, it cannot be undone. The genie cannot be put back into the bottle.

Risk assessment/AOP
MODULE AIM
To illustrate what is risk assessment
MODULE OBJECTIVES
Conduct a dynamic risk assessment
Explain relevant risk reduction mearsures
Identify pre/post mitigation levels

3 Risk assessment/AOP notes

Actions on Planning (AOPs)

Actions on planning, or AOPs, is a term that means there is a pre-planned procedure and method for reacting to and dealing with emergency situations. It is worth remembering the old saying that 'prior planning prevents poor performance'.

People often ask why should I bother planning for an emergency that is unlikely to happen? The point is that emergencies happen on a daily basis, and it may only be a matter of time until your location or building suffers from such an incident. With the increase in global terrorism the threat to us all is on the increase so we need to be prepared in case we become the focus for an attack.

Having plans in place to deal with a situation, prior to it occurring enables you and your team to rehearse and practice responses, so that in the unlikely event a situation does arise you will be ready to respond. Also by knowing what to do you can react much more quickly and save time and, particularly in medical emergencies, saving time saves lives.

Failure to plan may result in:
Injuries
Loss of income
Closure of business
Compensation claims
Criminal Prosecutions
Negligence claims

It is often asked, what is the need for planning for a terrorist attack or emergency when it is highly unlikely to happen? Failing to properly plan for a potential incident may result in failure to react if it occurs.

Furthermore there are certain key legal obligations that your employer or organisation must meet, and proper emergency planning can help, in part, to fulfil these requirements. All of the following acts and regulations underline an employer's legal responsibility to ensure safe working practices and procedures:

- Health and Safety at Work Etc Act 1974
- Management of Health and Safety at Work Regulations 1999
- Health & Safety at Work Regulations 1992
- The Occupiers Liability Act 1957
- The Employment Rights Act 1996

The Health and Safety at Work Etc Act 1974 also states that all members of staff have a 'duty of care' to take reasonable precautions and care to prevent and avoid injury to themselves or others.

As we discussed part of this responsibility involves having emergency or contingency plans in place to deal with these possible situations. Also it must be ensured that these plans are maintained and regularly reviewed, as well as ensuring that all staff members are aware of the plan and their role.

It is also advisable, if possible, to have drills or rehearsals where you can simulate a situation. This helps to highlight potential issues which need resolving within the plan, but also familiarises you and other employees with the procedures.

AOPs can help to successfully resolve a wide variety of situations, such as medical emergencies or power failures, not just a terror attack or threat.

For any action plan, regardless of the situation, it is vital that everyone is aware of their role in the plan and what is expected of them, no matter how small or large their role. So ensure that all key staff and personnel know their role and duties within the plan.

When an organisation, or individual, is preparing an AOP you will need to consider a wide range of information varying from the type of organisation, building layout, your clientele to the location of your building. All of these will affect your final plan and procedures.

Action plan
Each needs to know their role
Management staff
First-aid staff
Fire wardens
Security staff
Key personnel
Local emergency officials
All employees

Areas of consideration

An AOP looks at the bigger picture and all areas and aspects of an emergency and how to respond, but to simplify the process all of the information and resources can be broken down, and tackled piece by piece, and divided into the following three key areas of concern:

1. Threat identification and management

2. Risk reduction measures

3. Incident management

1. Threat identification and management

The most important point to remember is that failing to correctly identify the perceived threat to your location means that you can not create a concise AOP. So it is vital to look at every aspect of the threat your location and organisation faces. Only once you have gathered sufficient information will you be able to correctly weigh up your threat level, so you must examine at least the following issues:

National threat levels	
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

National threat level

- What is the current national terror threat level?
- Check the Home Office website for this information

Business practices and relationships

- What other organisations or businesses or groups does your organisation work with or support?
- You may be targeted due to their activities or profile

Risk Assessments

- What roles, functions, jobs or tasks do you and your colleagues/staff perform?
- These duties might make them and you a potential target

Black mail or threats

- Has your organisation received any blackmail/threats either via phone or mail?

Political or Religious affiliation

- Your organisations, as well as individuals, political or religious affiliations might raise the level of threat you face

Flight	Destination	Time	Gate
EK406	CHRISTCHURCH	0815	10
CZ321	SYDNEY	0820	11
QF010	SYDNEY	0825	7
QF129	SYDNEY	0835	4
AO7867	DENPASAR	0850	9
CX134	HONG KONG	0855	6
NZ192	CHRISTCHURCH	0900	2
DJ062	CHRISTCHURCH	0910	14
QF033	AUCKLAND	0920	1
NZ122	AUCKLAND	0930	5
EK404	AUCKLAND	0935	10
QF035	CHRISTCHURCH	0935	4
SJ722	DUNEDIN	0935	12
QF179	TOKYO	1005	3

Intelligence or warnings received

- Have you or the Police received information that your location or organisation is a potential target or on a terror hit list?

Type of location

- What kind of location is your workplace?
- Transport centres such as airports, train and underground stations have recently become high profile targets
- Infrastructure targets – power stations, gas mains or water plants have all been prime targets in the past

Soft/hard target

- Is your venue perceived a soft easy target such as many public areas due to high through traffic?
- Or is your venue already a hard target which is well secured and difficult to attack?

Previous incidents

- Has there been previous threats or attacks at your location?

Clientele or customer base

- Your organisation or business may not be the target, but it may well be that your customers are

Disgruntled employees or customers

- Frequently attacks are perpetrated by either former employees, often unhappy with the termination of their employment or other issues, or by angry customers as in the case of the Mardi Gras bomber, Edgar Pearce

Media attention

- Has your location or organisation recently received media coverage?
- This might highlight your site to prospective attackers

2. Risk reduction measures

- Identify the risks and hazards
  - Survey your workplace and decide what could reasonably be expected to cause harm.
  - Consult with employees about anything that they may have seen which is not immediately obvious to you.
  - Have a look at previous accident/incident report books to help you identify less obvious or recurring hazards
- Determine who might be harmed, and the level of potential harm
  - Customers and members of the public – could they be harmed by your activities?
  - Sharing of the workplace – how could your actions affect others in the workplace?

- Ask staff for anything they think you may be overlooking. In particular irregular duties or functions of their role.
- Are there workers with any particular requirements or needs whose safety may be jeopardized?

- Evaluate the risks and decide on precautions to take
  - Can I eliminate the hazard altogether?
  - If not, how can I control or reduce the risks to minimise harm?
  - Can I prevent access to the hazard? By sealing off the area or guarding the hazard.
  - Can I provide any welfare facilities? First Aid or washing facilities.
  - Have I involved staff, to ensure that the actions I have taken will work in practice and not cause further safety hazards?

- Record your findings and implement them
  - A proper check was made.
  - You asked who might be affected.
  - You dealt with all significant hazards, taking into account the number of people who could be involved.
  - The precautions are reasonable.
  - The remaining risk is low.

- Review your assessment and update if necessary
  - Look at your risk assessment again, have there been any changes?
  - Are there any improvements you still need to implement?
  - Have your workers spotted any problems?
  - Have you learnt anything from accidents or near misses?
  - Ensure that your risk assessment is kept up to date

Review and improve on a regular basis, and immediately if there are any major changes to your staff or workplace.

Once you have identified what you believe to be the threats and risks to your location or work place you need to look at these potential risks and threats and take steps to tackle these issues.

Risk reduction
Proactive prevention steps
Policies
Revising working practices
Changing business links and relationships
Altering your locations physical layout
Moving location
Introducing increased security measures
Review risk assessments
Issue relevant PPE
Work in partnership with local agencies
Relevant training
Installation of CCTV

Bomb Threat Stand-Off Distances			
Threat description	Explosives capacity (TNT Equivalent)	Building evacuation distance	Outdoor evacuation distance
pipe bomb	5 lbs/2.3 kg	70 ft/21 m	850 ft/259 m
suitcase bomb	50 lbs/23 kg	150 ft/46 m	1,850 ft/564 m
small car	500 lbs/227 kg	320 ft/98 m	1,500 ft/457 m
family car	1,000 lbs/454 kg	400 ft/122 m	1,750 ft/533 m
small van/minibus	4,000 lbs/1,814 kg	600 ft/183 m	2,750 ft/838 m
delivery van	10,000 lbs/4,536 kg	860 ft/262 m	3,750 ft/1,143 m
removals lorry	30,000 lbs/13,608 kg	1,240 ft/378 m	6,500 ft/1,981 m
articulated lorry	60,000 lbs/27,216 kg	1,500 ft/457 m	7,000 ft/2,134 m

Pre/Post mitigation levels

Incident Management
This should include the following:
Evacuation procedures
Setting up a control point
Have in place a command structure
First Aid officers and procedures
EMS liaison officer
Search procedures
Location security

3. Incident management

This is the point where your primary risk reduction measures have not prevented a situation and you now have to deal with an event. In any incident management plan it is important that the incident managers are fully familiar with the plan and put it into place without delay.

It is vital that you have in place an effective incident management structure and plan to respond to a bomb threat, discovery of an IED or an actual terrorist attack.

Evacuation planning

As mentioned earlier evacuation planning and training should be part of your AOP. You might need to evacuate your premises because of:

- A threat aimed directly at the building
- A threat aimed at the employer or their employees
- A threat received elsewhere and passed on to you by the police
- Discovery of a suspicious item in the building (perhaps a bag, postal package, an unclaimed hold-all or rucksack)
- An incident to which the police have alerted you

Whatever the circumstances, you must inform the police and emergency services as soon as possible of what action you are taking. The biggest dilemma facing anyone responsible for an evacuation plan is to how to judge where the safest place might be. For example, if an evacuation route takes people right past a suspect device outside your building, or through an area where you believe the device to be, evacuation may not be the best course of action (you might have to consider the use of protected spaces).

A general rule of thumb is to find out if the device is external or internal to your premises.

- If it is within the building you may consider evacuation, but if the device is outside the building it may be safer to stay inside
- The decision to evacuate will normally be yours, but the police will advise
- In exceptional cases they may insist on evacuation, although they should always do so in consultation with your staff and management

Planning and initiating an evacuation is a fundamental part of your AOP preparation, and should be done in conjunction with your management team. Depending upon the size and the location of the building, the plan may include:

- Full evacuation outside the building
- Evacuation of part of the building, if the device is small and thought to be confined to one location (e.g. a letter bomb found in the office room)
- Full or partial evacuation to an internal safe area, such as a protected space
- Evacuation of all occupants apart from designated searchers

All members of staff must be fully aware and trained in your organisations evacuation procedure as well as being aware of their role in such an incident. Also all evacuation exits, routes and muster points must be well defined. When formulating your evacuation policy and procedure you must take into consideration the following information:

- Appointed personnel to ensure that all occupants of the building are evacuated
- Appoint people to act as marshals at the assembly area
- Consider the location of the assembly areas, is it far enough away from the potential blast area (see BATF guideline chart)
- In the case of most vehicle bombs, for instance, this distance would put them beyond police cordons – although it would be advisable to have an alternative about 1 km away
- Disabled staff should be individually briefed on their evacuation procedures

What should you do?

You must establish and rehearse your bomb threat and evacuation drills. Remember to vary the type of threat and the location of the suspected device when performing these drills.

The design and layout of your building may play a great part in formatting your evacuation procedure, as staff may be safer in windowless corridors or basements than outside depending upon the type of device and its location. Assembly areas for staff must take account of the proximity to the potential threat.

You should bear in mind that a device delivered to the inside of your venue could have a far greater destructive effect on the structure than an externally detonated device.

- Agree your evacuation plan in advance with the police and emergency services, the local authority and neighbours
- Ensure that staff with particular responsibilities are trained and that all staff are drilled
- Remember, too, to let the police know what action you are taking during any incident

Control point
Information for emergency services
Missing personnel
Time of the discovery or explosion
Injuries sustained
Location of device or explosion
Special risks concerning the building
Other escape routes and muster points
Fire and alarm panel locations

Set up a control point

It is important that you build into your plan the creation of a control point, this helps with coordinating all activities as well as providing the emergency services with a central point of contact. The EMS (Emergency Services) liaison officer should be at the control point and have all the information that the emergency services may require from them such.

The location of the control point will vary depending upon the incident, but everyone should be aware of its position. All of the emergency services should be directed towards this point and any witnesses to the location of the device or the explosion should be present to give assistance or information as necessary.

Command structure

Once you have a control point and an EMS Liaison officer in place you will need to setup a command structure to ensure that tasks are performed and any instructions complied with.

This might involve having someone overseeing the following tasks

- Monitoring the first aid staff and injured persons
- Ensure no one returns to the building until safe
- Head count of all staff or occupants
- Communication between the groups
- Comforting individuals suffering from shock or fear

To this end Fire Wardens have already had training of evacuation procedures, so they may well prove to be the best people to take the head counts and ensure no one returns to the building.

First aid officers and procedures

In any emergency situation you will be aided and supported by the emergency services. However it is vital that until they arrive your First Aid officers are on the scene, and fully equipped, in case someone requires medical help before the medical services arrive on scene

EMS liaison officer

When the emergency services arrive on the scene they will need to be informed of everything that has happened so far. Also they will have certain directions that you will need to follow.

To enable them to perform their jobs more easily as well as ensuring clear lines of communication it is a good idea to designate someone as the EMS liaison officer. It will be their role to communicate with the emergency services your needs, as well as making sure that their directions are carried out by you and your colleagues.

Search procedures

If you suspect a device has been placed then you may need to implement a search procedure to locate the device, alternatively you may feel that you need to introduce searching of staff and visitors to ensure that no device enters your location.

There are numerous types and methods of searching that can be undertaken, and it is for each organisation and facility to determine which level of searching is suitable for them and their operation.

The SAFER approach	
S	Step back
A	Assess threat
F	Find help
E	Evaluate options
R	Respond

Adapted from the SAFER model © Maybo 2006

The SAFER approach

It is vital that if you are undertaking either routine searches or if you believe a device has been placed in your building then it is critical that any search procedure is undertaken in a way that doesn't place you or others in any undue danger. Maybo devised the SAFER dynamic risk assessment as a method of continuously assessing a situation so that individuals can recognise, assess and respond to

potential risks of violence. This risk assessment model can also be applied to the searching and discovery of a suspect device.

S = Step back

- Do not touch or disturb the device
- Don't rush in
- Physically step back, if possible – so you can see more and have a better chance of assessing the situation correctly
- Mentally and emotionally step back – remaining calm helps to keep your thinking clear and rational

A = Assess threat

- Identify the potential threat to your building and colleagues

F = Find Help

- Consider what help is needed to deal with the situation
  - Management
  - Security
  - Police
  - Do not attempt to deal with an incident on your own

E = Evaluate Options

- Examine what options are available to you to deal with the situation and select the most suitable one. These options vary depending upon the situation, but you generally have three main options:
  - Deal with the situation yourself – remembering to adopt a safe approach
  - Exit – leave the location due to the risk or dangers involved
  - Pass control of the incident to another person or organisation

R = Respond

- Once you have undertaken the above steps and determined what your options are, you must then respond to the situation, remembering to follow your organisations procedures

4Cs method

Can you remember the 4Cs?

1. Confirm
2. Clear
3. Cordon
4. Control

AOPs and the Emergency Medical Services

All, or any Actions on Planning (AOPs) from security staff, etc. should be approved by the local Police and Emergency Medical Services (EMS) and as 'civilians' our priority is to comply and assist the Police & EMS in any such incident effectively and confidently.

Identifying the Enemy

The basic ideology of al-Qaeda is that the world is divided into the true followers of Allah and the non-followers of Allah. This is why it has waged a holy war against the US and US allies. Some existing Muslim governments also fall within the category of enemy because they are considered traitors for maintaining friendly relations with the US.

Damage

Another principle of al-Qaeda is to achieve mass killings with their attacks. Their choice of targets reveal that no second thought is given to attacking soft targets, such as the public transport system, hotels and restaurants, where there are large numbers of civilians. al-Qaeda uses coordinated 'no-warning' suicide attacks. Therefore, it is difficult for the police to prevent such attacks in open and democratic societies.

Location security

In practise combining the security of a location and its every day business is a difficult task, particularly in today's unpredictable climate and the threat of IED attack.

If intelligence states that the location is a potential target for attack, due to the direct statement of the terror organisation or the associated ownership relationship with other 'high profile' organisations or individuals, then the incident manager might take the following steps:

1. After discussing with the management or owners consider closing the location, thereby denying the terrorist the target or limiting the potential threat to human life
2. Liaise with all the relevant emergency and local services as to any procedures you will need to know in the event of an incident
3. Inform and train all staff and management members on the requirements that must be put in place to increase the location security, and allow business to continue successfully
4. Implement any instructions from the emergency services and any policies directed from the building management

Location security can be broken down into 2 parts

1. Internal – inside the buildings
2. External – outside the buildings, car-parks and approach routes.

Internal security policy

All staff should be briefed as to the rules and regulations of any searching policies implemented by the building or location management for employees and visitors. All personnel should be briefed and trained on evacuation procedures and routes in the event of an incident, as well as the location of all muster points outside the venue in safe locations away from any potential blast distances.

Furthermore all personnel must be briefed as to what will be expected from them if the emergency services attend any incidents; this will range from medical personnel to maintenance personnel. The security of the building and occupants is the responsibility of all personnel, not just the security team or incident manager, and it is the job of everyone to ensure it is maintained.

National contacts list

National Counter Terrorism Security Office (NaCTSO)
Tel: 020 7931 7142
Web: www.nactso.gov.uk

Security Service
Web: www.cpni.gov.uk

Home Office
Tel: 020 7035 4848
Web: www.homeoffice.gov.uk

Anti Terrorist Branch
Hotline: 0800 789321

Preparing for Emergencies
Web: www.pfe.gov.uk

Association of Chief Police Officers (ACPO)
Tel: 020 7227 3434
Web: www.acpo.police.uk

Chief Fire Officers Association
Tel: 01827 302300
Web: www.cfoa.org.uk

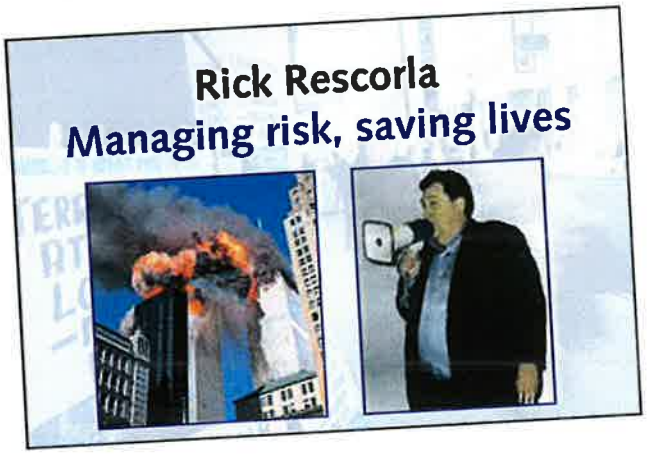
The Samaritans
Tel: 08457 909090
Web: www.samaritans.org

Victim Support
Tel: 0845 3030900
Web: www.victimsupport.org.uk

External security

Although there are numerous ways and methods of delivering an IED to its target location, they are most commonly placed either outside or close to the target location. This is obviously down to the decision of the attacker but usually this approach is chosen due to the lower chance of discovery by the intended targets.

Depending on your threat assessment and the existing threat level particular attention should be paid to where vehicles are allowed to park near the building or where visitors are allowed to alight from vehicles.
This is clearly a difficult judgement call as the functioning of the organisation and its accessibility requires a high level of planning by the individual preparing the AOP



All staff should be encouraged to report any suspicious sightings, to the designated person in charge of security procedures, allowing them to investigate and report any incidents to the emergency services.

Depending on the threat levels additional security measures should be taken, and potentially security personnel deployed at tactical locations away from the immediate perimeter of the location, this is to show a presence to any would be attackers and act as an early warning system, as well as a deterrent, and allows the incident management to initiate any in-place venue procedures and/or inform the emergency services.

It is essential for any plan to operate smoothly to establish and maintain a good working relationship with both public and the emergency services. Although the emergency services and any specialist agencies, such as bomb disposal units, will possibly require the assistance of venue security personnel, it is unrealistic to expect those agencies to divulge their tactics and procedures to outside agencies as this may hinder their own lives and their internal tactics.

4 Post incident module notes

Post incident considerations

So far we have looked at the history of terrorism, what is an IED and how to plan for dealing with a suspect package or a terror attack. But what happens after such an attack?

All organisations have to ensure that they provide their employees with the support they need in order to carry on performing their role but also to support them in times of stress and, in particular, after an incident has taken place.

This provision of support has several key benefits

- Helping staff deal with the situation
- Learning from the incident
- Staff feel valued and supported
- Rebuilds and maintains the morale of individual staff members and teams

Post incident victim support

In the most cases support for a victim is provided by their line manager, Personnel or Human Resources Departments, and there are three key points at which this support is crucial:

1. Immediately after the incident has happened

2. During any absence from work

3. Preparing for and returning to work

1. Immediately after the incident has happened

After any evacuation or attack everyone's first consideration must always be for the health of any victims. They may need urgent medical treatment and this must always take priority over any other considerations. You should ensure that they immediately get see by a trained and appointed First Aider, ambulance paramedic or doctor.

You must remember that after most incidents, a victims initial reaction tends to mainly be emotional and they will frequently show signs such as shock, confusion, anger, fear, disbelief, embarrassment and often they say how feelings of have a feeling of been violated.

At this early stage you need to acknowledge those feelings and allow the victim to express them. So allowing the victim to talk to you or others about their feelings and discuss how the incident has made them feel, is a vital part of providing them with the support and help that they need.

It is important for you to talk to the victim to try and establish what support they need. The following model is a good guide to identifying the support required.

Post incident support

MODULE AIM

Demonstrate post incident support

MODULE OBJECTIVES

Outline the benefits for supporting staff

Explain what you need to consider for post incident

Initial contact

- Identify if victim has injuries which need treatment
- Inform victim of the purpose of the meeting, which is to ensure they are OK and discuss their support needs

Listen to victim

- Actively listen to the victim without making judgments
- If victim does not want to discuss the incident do not pressure them to
- Victim may need to speak to the police, particularly if a serious or major crime has taken place

What does the victim need?

- Transport to hospital, doctors or home
- Contact family or friends
- Time off to recover
- Reducing stress and problems for the victim enables them to deal with their emotions and reactions more easily

Providing information

- **Let the victim know that their feelings and reactions are normal and to be expected, it can help to outline some of the reactions that may feel as time progresses**
- Details of sick leave
- Provide them with details of the organisations counselling or support scheme

Conclusion and next meeting

- Finally check if they need anything else and make the arrangements to get them home, etc.
- Arrange contact in the near future to ensure they have everything they need

2. During any absence from work

In most organisations the initial support is very good, but victims often say that they have no contact in the days after the incident. It is important to make an arrangement to see or speak to victims again with a few days. It is also important to keep in regular contact whilst they are absent from work to ensure they are recovering well. This contact can vary and depends on the needs of the victim, but it may include personal visits, emails or telephone contact.

Incident analysis

Obviously after an incident you must ensure that the corporate reporting procedure is followed, as this will allow you to examine the incident. This must be completed, by the victim, as soon as possible after the incident.

Every effort should be made to attempt to get the victim to complete the report, or at least the basic requirements, whilst it is fresh in his or her memory.

This reporting allows us to understand and review the incident and gives us the chance to actually work through the incident and learn from it.

It must be stated that you must be careful not to turn this process into an exercise to 'blame' those who could have prevented the incident or have been victims of the incident, as this will affect their morale as well as their recovery from any injuries sustained.

If the police are involved in a criminal investigation due to the incident it is important to seek their advice before you hold any form of incident review process, as they may wish to question you and your colleagues and take their statements first.

The learning review

A learning review is a simple tool that can be used to help you to understand and learn from an incident. By performing this exercise you will be able to identify areas that need improvement or procedures that are ineffective and need reviewing or amending.

The first step in the process is to get everyone to describe what happened during the incident. It is important that all parties have this opportunity to tell their version of events and what they saw, heard, felt and thought. This process helps the staff members involved in the situation to better understand the roles that others played and also helps to avoid people making assumptions about why a colleague did or did not do something.

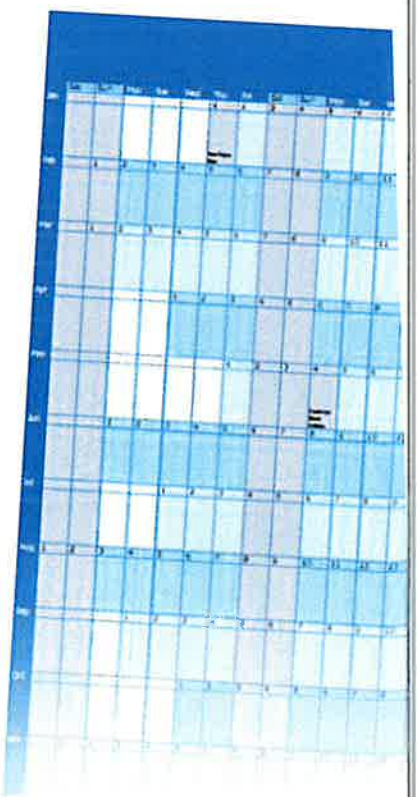
The next step is to look at the reasons why things happened the way that they did. This can show up any operational issues, for example outdated risk assessments. The final part is to identify what you have learnt from the process and attempt to find alternate ways of preventing or responding to a location.

3. Preparing for and returning to work

This is a complicated issue and has certain legal implications, both under employment law and contractual terms, and is best handled by either your management or personnel team.

Often a victim's return to work takes place quickly and with little apparent difficulty. However this is not always the case, and he or she may have a lengthy period of time off work to recover from their injuries and the mental effects of the incident.

It is important not to over react and become too protective, but equally important is the need to deal with any issues sensitively and supportively.



Return to work

Some people will want to return to work with the minimum of fuss whereas others might want more help. These different needs should be respected and all staff members need to avoid being overly protective towards the victim.

If a victim expresses some doubts about his or her ability to cope upon their return then a range of options can be considered:

- Working with a colleague – this can be very helpful by allowing the person to do their job but have the support of someone else until his or her confidence returns
- Gradual introduction – bringing them in initially on quieter or slower shifts to allow them to build up their confidence
- Spending time with the victim – you may spend more time with the victim in the first few days of their return to work

The first few weeks

In most cases, the return to work will be completed successfully and the victim will quickly return to his or her normal working duties. On the other hand, a victim may, for example, avoid duties or circumstances, particularly the duties that they were performing when the incident took place.

The victim may not even be aware of this behaviour and they might require extra support and time in such circumstances. As a supervisor or manager you should have an informal meeting within a few weeks of their return to work to ensure that they feel fully recovered from the incident and to check if any further support and help is needed.

Other post incident issues

There are always numerous post incident considerations and they vary massively depending upon the type of attack, location attacked, injuries sustained as well as the perceived on going threat.

Post incident issues
Proactive prevention steps
The clear up operation
How to return to business
Criminal investigation
Media interest
Insurance claims
Loss of revenue
Alternative work venue
Alternative accommodation
Future security
Risk reduction
Close of business

Appendix 1: chemicals and agents used in an CBR attack

Dirty bomb
Contains a mixture of explosive and radioactive material
Explosive material scatters radioactive dust and debris causing contamination
Causes serious injury and damage to property
Radioactive dust can pose a danger to health
Symptons of high-level radiation: nausea, diarrhoea, swelling and redness of skin

Anthrax
A serious disease caused by *Bacillus anthracis*
Spread by spores from infected products and inhalation
25–30% of cases are fatal
There are 3 types:
1. Skin (cutaneous)
2. Lungs (inhalation)
3. Digestive (gastrointestinal)
Symptoms:
Sores and blister, nausea, diarrhoea, or fever and flu-like symptoms

Plague
A disease caused by *Yersina pestis*, a baacterium found in rodents
Spread by flea bites, direct contact and inhalation
Mortality rate of around 30–60% if left untreated
It manifests in 3 main forms:
1. Bubonic (flea bite)
2. Septicaemic (bloodstream)
3. Pneumonic (respiratory)
Symptoms:
Fever, weakness, pneumonia, vomiting, abdominal pain, bloody sputum, shock and sudden death

Smallpox
An acute disease caused by the *Variola* virus
Spread by contact from lesions that ulcerate and coughing
Mortality rate of around 30%. 65–80% are left scarred
There are 2 main forms:
1. Variola major
2. Variola minor
Symptoms:
Fever, headache, prostration, back and abdominal pain, followed by rashes

Botulism
A serious muscle-paralysing toxin – the bacterium *Clostridium botulinum*
Spread by spores from infected products and inhalation
Fatal in 5–10% of cases
There are 3 types:
1. Food borne
2. Infant botulism
3. Wound botulism
Symptoms:
Fatigue, weakness, vertigo, blurred vision, paralysis of muscles

Cyanide
A deadly, rapidly acting chemical, in gas or crystal form
Exposure by contaminated air, water, food or soil
Fatal in 5–10% of cases
There are 3 types:
1. Food borne
2. Infant botulism
3. Wound botulism
Symptoms:
Restlessness, increased respiratory rate, giddiness, palpatations and convulsions

Mustard gas
Sulphur mustard is a blistering agent, introduced in World War I
A powerful irritant that damages the eyes, skin and repiratory tract
Fatal in fewer than 5% of cases
Exposure of skin and eyes to gas and inhalation
Symptoms:
Skin – redness nad itching
Eyes – irritation, pain, tears
Respiratory tract – sneezing, runny or bloody nose, breathlessness and coughing
Digestive tract – pain, diarrhoea, nausea and vomiting

Ricin
A poisonous byproduct from the process of making caster oil
A powerful irritant that damages the eyes, skin and repiratory tract
Deadly, if the dose is high enough. Death occurs during the first 3–5 days
Injection, swallowing or inhalation
Symptoms:
Inhalation – breathiing difficulties
Ingestion – vomiting, diarrhoea
Skin and eye exposure – redness and pain

Sarin
A nerve gas, colourless and tasteless, developed from a pesticide
A powerful irritant that damages the eyes, skin and repiratory tract
Repiratory failure can lead to death
Exposure to the liquid or inhalation of the vapour
Symptoms:
Small dose – Watery/painful eyes, repiratory problems, vomiting, diarrhoea, urination, headache, confusion, increased heart rate and blood pressure
Large dose – convulsions, paralysis, unconciousness

Appendix 2

Best Practice Action Plan	Yes	No
Are empty or unused offices, rooms or areas kept securely locked?		
Are only authorised vehicles allowed access to parking areas?		
Is there regular checking and monitoring of all public access areas?		
Do all staff and visitors wear ID badges when in your building?		
Is the potential to hide devices limited in public areas?		
Are outside places, entrances, stairs and public areas kept safe, clean and tidy?		
Do the entrances and emergency exits of your building restrict unauthorised access?		
Are visitors escorted at all times whilst on the premises?		
Are staff encouraged to report any suspicious packages, objects or behaviour?		
Are you informed of your buildings emergency and evacuation procedures?		
Do you know your role in an emergency evacuation?		
Do you know where your appointed evacuation or gathering point is situated?		
Does your building use operational real time CCTV?		
Is your CCTV system detailed enough to identify people?		
Do the recorded CCTV images include the time and date?		
Do your premises operate a search policy, to personnel, bags or vehicles?		
Do your premises have a regular search for suspicious and unidentified packages?		
Does your building have its own security team?		
Are your evacuation routes and assembly points checked before use?		
Do you have a security policy that details all relevant security procedures?		
Is this policy regularly reviewed and updated?		
Do you know the contact details for your local Counter Terrorism Security Advisor?		
Do you have regular drills and rehearsals for evacuations and emergencies?		

If you have answered 'No' to a question then you should examine the issue in question and seek to address this security area as soon as possible.

If you are unsure whether to answer 'Yes' or 'No' you should check with the person responsible for security or safety in your organisation or building to find out the relevant information. This will help to ensure that you are aware that the issue is being dealt with, also it will highlight the fact that this information is not being shared within the organisation.

Even if you have answered 'Yes' to a question it is vital to remain alert to these issues and constantly review your security and safety measures to ensure they are effective.

Skills for Security Ltd
Security House, Barbourne Road, Worcester WR1 1RS
phone: +44 (0)8450 750111 fax: +44 (0)1905 724949

e-mail: info@skillsforsecurity.org.uk
web: http://www.skillsforsecurity.org.uk

in association with

Rutherford Training Consultants
Suite 16 Boundary House Business Centre, Boston Road, London W7 2QE
phone: 0208 434 3573, 0208 434 3574 fax: 0208 434 3527

e-mail: info@rtc-training.co.uk
web: http://www.rtc-training.co.uk