Play Training Module

This is a transcript of a narrated multimedia training module. You can view the online Multimedia training module by clicking the link above or at riskcentral.com.au

Terrorism Awareness

for critical infrastructure sites

and other sites at high risk of terrorist attack

Tony Matthews, B.E., M.B.A
Managing Director – Risk Central
Email: tony.matthews@riskcentral.com.au

Intended use of document: This text is intended to be used as training to improve general terrorism awareness of employees working at critical infrastructure sites and other high risk sites. The training is intended to be accessible publicly on line. The respective web site will also manage, record and track the training of groups.

1. Introduction

Welcome to this Terrorism Awareness training module. During the next 15 minutes you will learn how to identify suspicious behaviour and what to do when you see it.

This training is for insurance & information purposes only. This Training Module is a general course which covers important terrorism awareness issues. It is not a comprehensive guide and does not ensure compliance with any standards, regulations or statuary obligations and does not cover all conditions, situations, causes or controls.

Rather the module targets important issues and concepts, in order to keep the training brief, practical and effective. Please note that effective controls will reduce risk, but will not eliminate it. Risk management should therefore be seen as an ongoing "Continuous Improvement" process.

 © Risk Central Pty Ltd

This module is mostly a collection of publicly available information sourced from a number of different government security agencies around the world. For more information on terrorism risks and controls please see the websites of the government agencies referenced throughout this training module and other appropriate references.

- Section 2 of this Training Module explains how to identify suspicious behaviour,
- Section 3 outlines specific indicators for potential vehicle or boat bomb attacks,
- Section 4 discusses what actions you should take if you are aware of suspicious behaviour,
- Section 5 explains how to identify suspicious behaviour in work colleagues or contractors,
- Section 6 provides examples of materials which maybe used around your workplace to promote increased awareness.

2. Suspicious behaviour

The fight against terrorism requires you to be aware of and report suspicious behaviour. Terrorists try to blend in and assimilate with their surroundings. Most terrorist acts are well organised and well planned. Comparing reports of suspicious behaviour helps authorities to identify potential threats and act to prevent terrorist attacks. Therefore your assistance in reporting suspicious behaviour may help stop a terrorist attack.

This training module attempts to promote the reporting of suspicious incidents by helping people identify indicators, characteristics and behaviours that may reveal terrorist activity. Any single indicator described below is not cause for alarm. The totality of circumstances must be considered when making a decision to report activity to your local authorities. But if in doubt, remember that you probably know your workplace best. So, use your common sense, follow your instincts and err on the side of reporting. Prompt reporting of suspicious activities may prevent a terrorist attack.

This material includes information which has been summarized, paraphrased or copied from publicly available material sourced from the Miami Police Department.

Potentially Suspicious Behaviour and Activity

Certain kinds of activities can indicate terrorist plans that are in the works, especially when they occur at or near critical infrastructure, high profile sites or places where large numbers of people gather – like government buildings, gathering places, bus or train stations, Airports, utilities, major public events, Ports, or military facilities.

Potentially suspicious behaviour or activity includes:

 © Risk Central Pty Ltd

Surveillance

Anyone recording or monitoring activities, taking notes, using cameras, maps, binoculars, and such, near a key facility or an event. Specific surveillance techniques may involve multiple sightings of the same suspicious person, activity, or vehicle.

Suspicious Questioning

Anyone attempting to gain information in person, by phone, mail, e-mail, and such, regarding a key facility, event or people who work there.

Tests of Security

Any attempts to penetrate or test physical security or procedures at a key facility or event.

Acquiring Supplies

Anyone attempting to improperly acquire explosives, weapons, ammunition, dangerous chemicals, uniforms, badges, flight manuals, access cards or identifications for a key facility or event or to legally obtain items under suspicious circumstances that could be used in a terrorist attack.

Suspicious Persons

Anyone who appears out of place in the area, neighbourhood, workplace, business establishment or near a key facility or event.

Dry Runs

Any behaviour that appears to be preparation for a terrorist act, such as mapping out routes, playing out scenarios with other people, monitoring key facilities or events, timing traffic lights or traffic flow, or other suspicious activities.

Deploying Assets

Have you observed abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility or event. This includes suspicious objects, bags or packages, in suspicious places. You know your workplace best and you know when something is out of place.

This material includes information which has been summarized, paraphrased or copied from publicly available material sourced from the US Department of Homeland Security, US FBI and the Miami Police Department.

© Risk Central Pty Ltd

3. Vehicle and boat bombs

Certain kinds of activities can indicate terrorist manufacture of a car, truck or boat bomb. Potentially suspicious behaviour or activity includes:

- Theft of explosives, blasting caps, or fuses, or certain chemicals used in the manufacture of explosives.
- Rental of self-storage space for the purpose of storing chemicals or mixing apparatus.
- Delivery of chemicals directly from the manufacturer to a self-storage facility or unusual deliveries of chemicals to residential, water side or rural addresses.
- Chemical fires, toxic odours, brightly coloured stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
- Modification of a car, truck or van with heavy duty springs to handle heavier loads.
- Unusual modifications of a boat.
- Small trial explosions in rural areas.
- Treatment or existence of chemical burns or missing hands / fingers.

This material includes information which has been summarized, paraphrased or copied from publicly available material sourced from the Miami Police Department.

4. What should you Do

Any single indicator is no cause for alarm. The totality of circumstances must be considered when making a decision to act on or make a report to your local authorities. But if in doubt, remember that you probably know your workplace best. So, use your common sense, follow your instincts and err on the side of reporting. Prompt reporting of suspicious activities may prevent a terrorist attack.

You should report the incident to local authorities. This normally means reporting to site security, they have been trained to handle these situations. Alternatively, if site security is not available, contact police on an emergency number (ie 000) if you feel the situation is urgent or contact the Australian National Security Hotline on 1800 123 400 if the situation does not appear urgent.

You should not approach or engage a suspicious person unless you feel that it is safe and you feel comfortable doing so. If you do approach a suspicious person you should do so in a non confrontational and polite way. For example – asking “If they require any help?” or “Can I enquire as to your business here?”

If you notice something which maybe suspicious you should note down a description even if you are not sure you are going to make a report. You can decide about making a report after you have made some notes.

 © Risk Central Pty Ltd

If you notice an object you suspect could be a bomb, report it to site security. Do not touch the object and do not use your mobile phone or radio, as these items can set off explosive devices.

The following points will help you to describe suspicious behaviour to authorities:

Describing Suspicious Behaviour:

- WHO did you observe?
- WHAT did you see? Be specific.
- WHERE did you see it?
- WHEN did you see it?
- WHY is it suspicious?

Try to be:

- ACCURATE
- FAST
- COMPLETE

About the Person:

- Sex
- Race
- Age
- Height
- Weight
- Build (thin, medium, heavy set)
- Hair
- Complexion (light, dark, olive)
- Accent
- Special Features (scars, tattoos, missing teeth)
- Clothing (head to toe, colour, style, defects)
- Weapons
- Method of escape (direction, vehicle, etc)

About the Vehicle:

- Number Plate (most important)
- Year, make, model & colour
- Body type
- Passengers in car
- Damage, markings or anything unusual

This material includes information which has been summarized, paraphrased or copied from publicly available material sourced from the Miami Police Department.

 © Risk Central Pty Ltd

5. Suspicious employee behaviour (Optional)

Some external threats, whether from terrorists, criminals or competitors seeking a business advantage, may rely upon the co-operation of an insider. This could be an employee, contractor or agency staff (eg cleaner, caterer, security guard) who has authorised access to your premises. Much of the control for this issue is provided by good basic recruitment and employment practices such as identification, past employment, reference, qualification, immigration and criminal background checks.

Other controls rely on the ongoing awareness of employees and managers. Managers and staff should be alert to anything unusual in employees' behaviour or attitudes. Any information should be handled sensitively and confidentially. Whatever the circumstances, control measures should be clearly proportionate to the perceived terrorism risk. Employees should be informed of these risks and how they may be controlled. Note that any action taken as a result of such concerns must be in accordance with employment law.

Information security policies can assist to prevent or minimise access to sensitive information by persons who do not have a need to know, and may provide an ability to track who has accessed the information. Permit access to sensitive locations, assets or information only to those who genuinely need it.

Unusual behaviours or attitudes may include:

- Gambling, drug or alcohol problems.
- Expression of support for violence-prone views, actions or incidents.
- Major unexplained changes in lifestyle or expenditure.
- Sudden loss of interest in work, or overreaction to career changes or disappointments.
- Manifestations of stress such as over-emotional behaviour.
- Unusual interest in security measures or area of work outside the norm.
- Changes in working patterns, for instance working alone or at unusual hours, failing to take holidays.
- Frequent unexplained absences.
- Repeated failure to follow recognised procedures.
- Unusual travel abroad.
- Relationships with or support for individuals or institutions that are generally regarded as suspect.
- Sudden or marked change in religious, political or social affiliation or practice which has an adverse impact on the individual's performance or attitude to security.

Any single indicator described below is no cause for alarm. The totality of circumstances must be considered in any specific situation.

 © Risk Central Pty Ltd

Contractors and Agency Staff

The use of contractors and agency staff for many services (e.g. IT support, cleaning, catering, security guarding and consultancy) can create additional vulnerabilities and expose businesses to greater personnel security risks. While some agencies may be careful in their selection procedures, the less rigorous are open to exploitation by terrorists and sympathisers. Therefore, you should:

- Make it a contractual obligation that contractors validate the identities and backgrounds of their staff.
- Conduct regular monitoring of contractors' compliance with the contract.
- Establish that each contractor is part of a recognised professional organisation responsible for accrediting standards in that industry.
- Confirm that the individual sent by the contractor or agency is the person who actually turns up. For instance, ask the contractor to provide an authenticated photo of the individual, together with their full name, in advance of arrival. Ask the individual to provide photo identification that can be checked on entry.
- Provide photo passes to contract staff, once you are satisfied that the person who turns up on the day is genuine. The pass must be worn at all times. Ideally, the employer should retain the pass between visits and hand it over only once the photo has been checked.
- Encourage employees to be sceptical of anyone not wearing the appropriate ID.
- Have a procedure for substituting contract staff with temporary replacements when the usual contract staff are away or ill; consider whether the replacement's duties or access need to be restricted.
- Supervise where possible contract staff whenever they are on the premises and particularly if they have access to sensitive areas.
- Nominate a permanent member of staff to be responsible in personnel terms for contract staff (i.e. not merely for overseeing delivery of the contract), so that potential security problems may be identified and addressed early.

This material includes information which has been summarized, paraphrased or copied from publicly available material sourced from the UK MI5.

© Risk Central Pty Ltd

6. Posters & references

Congratulations on completing this Terrorism Awareness Training Module. Please consult the references below for more information.

US Department of Homeland Security: www.dhs.gov/dhspublic/

US Federal Bureau of Investigation: www.fbi.gov/

UK MI5: www.mi5.gov.uk/

US Miami Police Department: www.miamidade.gov/

UK London Metropolitan Police:
www.met.police.uk/counter_terrorism/campaign_ct.htm

Australian National Security Government Site: www.nationalsecurity.gov.au

© Risk Central Pty Ltd