back to BASICS: Security

ABP Security Briefing Note 2015-2

Islamic State attacks in Grenoble, France and Sousse, Tunisa

Many of you will have seen the media reports of the attack last Friday 26th June where a man was beheaded and displayed at the entrance to a US-owned industrial facility in Grenoble, France and of the marauding firearms attack in the Tunisian resort of Sousse.

These attacks are the latest in a series of gruesome murders launched by Islamic State (IS) and their supporters in Europe following a statement published on the internet by Abu Mohammad al-Adnani who provoked a an overnight shift in the methods employed by so-called international terrorists.

Groups such as Al Qaeda (AQ) and their affiliates were very focused on the use of explosives and their delivery; person or vehicle borne devices with the latter preferred in order to delivery larger payloads and cause the maximum deaths and damage. IS differ from AQ in that they advocate low-tech violence against western civilians, ignoring many of the traditional targets such as stadiums, shopping centres and transport hubs – typical crowded places. These attacks, because of their spontaneous, easily armed (kitchen knives from supermarkets for example) and seemingly random nature make them almost impossible to prevent unless they are detected during the attack planning stage.

What is attack planning?

Attack planning, also referred to as hostile reconnaissance, is the work undertaken by a terrorist organisation before an attack in order that the perpetrators are successful. Often the attack planner is not directly involved in the actual attack and may be providing planning services for a number of terrorist actors involved in multiple scenarios.

Whilst difficult to detect, it is not impossible. The types of behaviour that suggest attack planning is being conducted are:

- Suspicious activity – the person looks out of place or is in a restricted area without ID/Hi-Viz
- Unusual questioning – the person is asking questions of staff to determine the security arrangements or find vulnerabilities in procedures in order to gain access
- Photography – taking photographs of unusual things such as security cameras, fences, gates and gatehouses, guards or other infrastructure that may be a target (passenger terminals or lock gates)
- Drawing plans or maps – making detailed notes and/or sketching site or building layouts
- Testing security arrangements – a person may set off a fire alarm, leave an inert but suspect package or attempt to gain unauthorised access to restricted areas in order to identify muster points and test the reaction times of security teams

You may consider a person to be suspicious by their appearance or demeanour. Acting aloof, constantly checking over their shoulder,

back to BASICS: Security

avoiding eye contact, acting or speaking nervously or having scant details when claiming to have an appointment.

Perhaps the person is wearing unusual clothing i.e. a heavy overcoat on a warm sunny day. Perhaps that person is using the coat to conceal something?

What can you do to assist?

Firstly, it is important to bear in mind that the UK intelligence services and law enforcement has not determined that a credible threat to the UK is preparing to carry out an attack. **There is no intelligence to suggest that the UK, or especially ABP, is the subject of attack planning at this time**. The purpose of this briefing is to **alert but not alarm**.

However, that is not to say that we should not be vigilant and should a person consider attack planning at our business locations, we should be ready to send a message – we will Spot It, we will Report It and we will Stop It.

But our security teams are few in comparison to the total workforce – that is why you are our eyes and ears. As with health and safety, we all have a part to play in protecting ourselves, each other and the business. You wouldn't walk past an unsafe act and risk your colleagues, why would you risk letting a trained and prepared terrorist group into your workplace?

There are a number of simple things you can do to improve the public impression of our security culture:

- Challenge those not wearing ID when required to do so
- Don't allow tailgating through security barriers/doors into controlled areas
- Lock your computer with CRTL-ALT-DEL every time you leave it unattended
- Do not give out sensitive information over the phone to cold-callers or to unknown visitors asking detailed questions
- Report suspect articles (bags/parcels) and follow instructions[1]
- Report anything you consider to be suspicious

We cannot overstate the importance of reporting anything you consider to be suspicious to either the Port Facility Security Officer or equivalent, security team and line-manager or, if an emergency, the local police via 999.

The above list of attack planning markers is not exhaustive and what you consider to be suspicious is subjective; different people will see normality where others will not. Whatever the circumstances our message is the same. If you think it is suspicious, tell someone and let security or the police decide if it is something to act upon.

If you have any suspicion that a member of staff is involved in or assisting others to conduct such criminal activity you can also report this anonymously via the Whistleblowing Hotline 0800 374 199.

Thank you for your continued vigilance and if you have any questions feel free to email security@abports.co.uk.

[1] See Security Briefing 2015-3 for further information