Situational Awareness: Oblivious or Aware?

Maintaining ongoing situational awareness can be challenging and there is a risk of missed opportunities to act if inadequate attention is paid to the threat landscape and warning signals aren't spotted. Andy Blackwell and John Wood of 3DAssurance examine the challenges caused by poor situational awareness and offer some practical solutions for front line staff to help increase their organisation's security defences and overall safety.

Situational Awareness is an individual's awareness of their surroundings. A similar concept applies to the organisation as a whole, reflecting the collective situational awareness of its people.

Four stages of Situational Awareness

We have developed a four-stage model of Situational Awareness, using a colour code system US Marine Colonel Jeff Cooper developed to teach situational awareness. Like the organisation, an individual's protection relies on Situational Awareness of safety and security.

White: "Oblivious"

You are relaxed and not paying attention to what is going on around you. Examples are when in surroundings assumed to be safe, such as at home, or when focussing on your mobile phone in the street. You have blind spots you are unaware of.

Yellow: "Aware"

You are relaxed but paying attention to what and who is around you. This should be your normal routine state and is the basis of your situational awareness.

Amber: "On Alert"

Something has caught your attention and increased your level of alertness. It might be a threat and you are already running through "what-if" scenarios to consider possible solutions.

Red: "Ready to Act"

You are ready to act, whether that is fight or flee. You may not actually have to, but you have made a decision that you are ready and willing to act, and you have decided what the trigger would be.

It is obviously desirable that all personnel be constantly Aware (Yellow), but that is not how the human psyche works.

People tend to be at their most security aware in the immediate aftermath of major terrorist attacks or other catastrophic events, but as time passes, memories of the atrocities fade, and situational awareness begins to wane. Staying alert is as much about addressing human blind spots as those created by inadequate positioning of CCTV cameras. Complacency and lack of situational awareness is a recurring theme in recommendations following inquiries into responses to terrorist attacks and other major disruptive events.

Complacency is not recklessness. It is not a deliberate choice, it is human nature for alertness to decline in the absence of constant visibility of the danger. Complacency is often referred to as the biggest risk of all, and the enemy of excellence. We see it compromising safety, security and more recently, public health. Businesses fail due to it, and lives are lost because of it, and like any other risk it needs careful, ongoing management.

Organisations and their people need to be imaginative in their approach to threat and risk management if they are to avoid complacency. The clearer they can imagine a particular risk materialising, the more likely they are to be able to develop robust responses to manage it. Psychologists explain that *failures of imagination* are due to our inability to confront threats that lie beyond our realm of experience, and since our minds evolved to deal with imminent threats, for most of us, there does not seem to be much attention to future, more abstract dangers. Leaders who fail to take risks seriously enough and neglect to promote a culture of safety and security are putting their people and organisations at risk of harm. This failure of management and failure of imagination were both identified in the 9/11 Commission Report as factors contributing to the terrorist's success.

The lead up and response to the Manchester Arena Attack, described by the inquiry chairman as a *litany of failures,* is the latest in a string of incidents involving complacency and missed opportunities to act. The attack took place on Monday 22nd May 2017 at 10.31pm when Salman Abedi, a suicide bomber inspired by the so-called Islamic State, detonated his rucksack bomb (which weighed more than 30 kg) in the City Room, close to one of the exit doors from Manchester Arena. The attack took place at the end of a concert by Ariana Grande, as concert goers were leaving the venue. 22 people were killed and hundreds more were injured. The bomber also died in the attack.

A member of the public who had voiced concerns about Abedi to a security officer minutes before the bombing was 'fobbed off'. Sir John said this was the most striking missed opportunity to act. It is ironic that *'See it. Say it. Sorted.'* the promise behind the slogan pioneered by British Transport Police (with the Centre for the Protection of the National Infrastructure and Department for Transport) as part of a campaign to increase public awareness and reporting of crime and potential terrorist acts was broken and the opportunity missed. The campaign has largely been a success, but is dependent on the public being confident that their concerns will be taken seriously.

The national threat level at the time of the bombing was assessed by the UK's Joint Terrorism Analysis Centre (JTAC) as *Severe* meaning that an attack was 'highly likely'. The UK's terror threat level had been at severe since the 29th of August 2014, apart from a short period when it was raised to critical following the Manchester Arena attack. The fatal Westminster attack near the Houses of Parliament in which 4 innocent people were killed occurred just two months earlier. Despite the recent history of attacks, security officers

deployed at the arena were lacking situational awareness. The report mentions that it is difficult to reach a safe conclusion about what the consequences of the missed opportunities were, if any, as no-one knows what Abede would have done had he been confronted prior to him detonating his device at 22.31.

Terrorists and other criminals need intelligence to conduct their nefarious activities. This can be gathered using a variety of methods, including basic research, hostile reconnaissance and surveillance of potential targets. It can include dummy runs, testing of security responses, and the use of insiders within the target organisation. Hostile reconnaissance is used by bad actors to identify targets, find weak spots and vulnerabilities in the organisation's protective security arrangements, and ascertain the type and level of security in place. Analysis of major terrorist attacks and plots reveals the importance terrorists place on gathering intelligence about their targets. Some notable examples include:

The Manchester Arena bomber who is said to have conducted three reconnaissance missions, but lack of security officers and inadequate training meant that there was "almost no chance" of spotting the bomber according to an expert witness at the subsequent inquiry.

The mass fatality terrorist attacks in Mumbai in November 2008, often referred to as India's 9-11, which killed in excess of 172 people involved detailed reconnaissance before the deadly attacks.

In January 2019, Ashiqul Alam admitted to purchasing a firearm for use in a full-scale, mass-casualty attack in Times Square, New York. Alam had conducted several reconnaissance trips to Times Square, and used his mobile phone to make a video recording of the area as he searched for potential targets.

On 31 December 2021, India's National Investigation Agency (NIA) conducted searches and arrested Arsalan Feroz, an operative of a terror group, in Srinagar in a conspiracy case related to radicalising, motivating and recruiting youths for terror activities. A senior NIA official said the accused had been recruiting individuals (overground workers) to carry out reconnaissance of pre-determined targets, co-ordinating and transporting weapons to support Lashkar-e-Toiba.

Bad actors are constantly on the lookout for 'attack opportunities', so we need to be careful of the 'security impression' our organisation is portraying. Is the organisation's security culture such that suspicious activities are immediately reported and responded to, or has complacency and stagnation set in and the security environment is lax? If there is inadequate security staffing, lack of detection equipment and a poor security culture evidenced by behaviours such as staff not visibly wearing identification cards, tailgating and slow responses to security alerts and alarms, a person gathering intelligence with hostile intent, will quickly be able to ascertain that the organisation is vulnerable and an easily target. Conversely, an organisation that projects strong security 'signals' is likely to deter or displace a potential attacker.

Hostile reconnaissance activity puts terrorists and criminals at risk of detection and is the greatest opportunity we have of disrupting bad actors and the opportunity is maximised by good situational awareness.

Three simple security measures will maximise the opportunity to disrupt bad actors

1. Using the front line properly

Front line security personnel play a significant role in helping to maintain the integrity of security. They are the eyes and ears on the ground, and are often the first person anyone comes into contact with when visiting the site. This provides them with an opportunity to spot unusual activity, such as hostile reconnaissance. Whilst there's no such thing as a typical terrorist or criminal, front-line security personnel are uniquely placed to get a good understanding of what is 'normal' behaviour within the environment, so behaviour falling outside the norm can be identified and investigated further. If something doesn't look or feel quite right, good security officers ask questions and trust their instincts. They are constantly at Stage 2 or 3 of Situational Awareness.

2. Engaging all staff

The security team also has a role as security ambassadors and exemplars of situational awareness.

"Security Culture" is perhaps an overused phrase that an effective culture really means all personnel being committed to their role in maintaining security. The example set by a respected security team plays a big part in gaining this commitment.

It means people demonstrating positive security behaviours by strictly comply with existing security arrangements. It means everybody remaining vigilant at all times; willing to challenge anybody not wearing a pass, honouring policies such as clear desk, pass wearing, pre-announcing visitors, and reporting anything suspicious. The importance of everybody being at Stage 2 of Situational Awareness is obvious.

Such behaviours present a formidable message with anybody engaged in hostile reconnaissance, as well as helping to prevent attacks.

3. Using a Security Management System

Organisations have many security measures in place. A Security Management System draws these together into a comprehensive and cohesive "system". This is not a software system, it is a formalised, risk-driven framework for integrating security into the daily operations and culture of the organisation. The SeMS enables an organisation to identify and address security risks, threats, gaps and weaknesses in a consistent and proactive way.

Amongst other things, the SeMS provides a means for managing threats, reporting suspicions and handling incidents. It ensures that all staff are aware of their security responsibility and helps develop an effective security culture throughout the organisation.

A good introduction to SeMS is the UK Civil Aviation Authority's "Framework for an Aviation Security Management System" available free on their website. Although written for aviation, it is universally applicable to any organisation that needs good security. Many of our previous TPSO articles also describe a SeMS.

Conclusion

Staying alert is as much about addressing human blind spots such as complacency, threat, and terrorism fatigue as those created by inadequate positioning of CCTV cameras. The military slogan *Complacency Kills* has relevance to security, reminding us that if we let our guard down, innocent people may die or be seriously injured.

We owe it to the victims of all terrorist attacks where failures and missed opportunities were identified, to ensure lessons identified become lessons learned and implemented.

The challenges going forward are complex, but implementing a recognised SeMS (such as CAP 1223) will provide organisations with the means to grow a positive security culture, break the recurring cycle of complacency and enable them to provide effective, efficient and assured security, using a proven framework. SeMS also provides a credible way forward for organisations seeking to fulfil their Protect Duty requirements.

References

Cooper's colours: A simple system for situational awareness	https://www.police1.com/police-trainers/articles/coopers-colors-a-simple-system-for-situational-awareness-Np1Ni2TbRj9EkGUN/
Blind Spot: Failure of Imagination and Existential Threats	https://www.psychologytoday.com/us/blog/our-evolutionary-selves/202003/blind-spot-failure-imagination-and-existential-threats
National Commission on Terrorist attacks on the United States – '9/11 Report'	https://9-11commission.gov/report/
Manchester attack: Bomber's 'hostile reconnaissance' missed due to poor training and lack of staff, inquiry hears	https://news.sky.com/story/manchester-attack-bombers-hostile-reconnaissance-missed-due-to-poor-training-and-lack-of-staff-inquiry-hears-12149345
Manchester Arena Inquiry Volume 1: Security for the Arena	https://www.gov.uk/government/publications/manchester-arena-inquiry-volume-1-security-for-the-arena
Assessing Hostile Reconnaissance and Terrorist Intelligence Activities	Kevin A O'Brien (2008), The RUSI Journal, 153:5, 3439, DOI: 10.1080/03071840802521903
CPNI Crowded Places Guidance: Hostile Reconnaissance	https://www.gov.uk/government/publications/crowded-places-guidance/hostile-reconnaissance
Framework for an Aviation Security Management System (SeMS) - CAP1223	Civil Aviation Authority: https://publicapps.caa.co.uk/CAP1223