Features

Aviation Security: A Crisis of Confidence by Andy Blackwell

December 18, 2019

In the near quarter century that I've been working in aviation security, I've seen significant changes to the threat landscape and the methods used by government and industry to keep the sector secure. I've been heavily involved in the responses to major terrorist attacks against aviation, including

received by the various organisations I've worked for. What remains abundantly clear is the unhealthy fascination terrorists, and others with sinister intent, have with civil aviation.

Attacks against the industry tick all the boxes on the terrorists' check sheet: causing mass fatalities and injuries, creating a climate of fear, and bringing about economic and reputational damage to the sector and those charged with protecting it. The enduring threats to the industry have also broadened in recent years, with cyber-attacks now a reality due to the increased connectivity of aviation operations. The perpetrators remain confident in their capabilities and readily exploit terrorist techniques used in conflict areas to conduct attacks elsewhere. Hostile drones, particularly those used in swarm attacks, are just one new form of attack we are likely to have to contend with, not to mention non-terrorist use for disruption purposes by single-issue protest groups. However, of all the threats the industry faces, hostile insiders present the most challenges. We ordinarily regard our people to be our greatest strength, but they can pose the greatest threat.

The significant 'target hardening' of the industry has largely resulted from a 'cat and mouse' game with those seeking to cause harm versus the protectors. Getting ahead of the game will always be a challenge despite the best efforts of regulators and industry.

The Invisible Threat

The threats I've mentioned are all well documented and visible. My security assurance work as a consultant has highlighted one significant concern relating to an invisible threat in many organisations, one of our own making which nevertheless poses a risk to the sector. It links to our response to threats and the messages we put out in the public domain, the content of which can be far from helpful. I've lost count of the number of times the 'line to take' from law enforcement, regulators or indeed industry itself has been along the lines of; 'acting out of an abundance of caution' and then goes on to describe what is far

if there ever was one in the first place. In some cases, there's also been a reference indicating that they knew the 'threat' wasn't credible. The use of such terminology shows that the organisation does not have confidence in its threat assessment and risk management processes.

This is not a good signal to be sending out. In addition to the adverse impacts this overreaction has on organisations and the public psyche, and the encouragement given to those seeking to harm the industry, it can fuel the egos of those involved in hoaxes and other disruptive activities. Imagine the buzz experienced by the hoaxer or copycat as they see a 'spectacular' response to their non-credible threat. In essence, the invisible threat is an undermining of deterrence activities and inadvertently offering encouragement to terrorists and hoaxers alike.

Causes and Unintended Consequences

From what we have seen repeatedly, lack of management insight into security risks is behind the 'rush' to an abundance of caution. Their lack of knowledge of their organisation's security performance and resilience results in them doing what they consider to be the lowest risk option. In reality, an abundance of caution creates a false sense of security.

Abundance of caution responses cannot be relied upon to be the safest response strategy, diverting aircraft to 'unknown' airports can increase safety risks, and evacuating areas unnecessarily can create stampedes and chaotic scenes which bring about additional safety and security risks. There are some notable examples of people suffering heart attacks after building evacuations. Abundance of caution approaches do not always provide the 'comfort blanket' that people mistakenly think they will.

Unnecessary overlaying of security measures gives the impression to the public that we can't get things right the first time around. Such duplication can also frustrate front-line security personnel who feel that there is little point in them

> "…an abundance of caution creates a false sense of security…"

Clearly there are times though when targeted, risk-based additional security measures are appropriate. It is the overcautious and ill-informed practices we are trying to eradicate. In terms of resource management, deploying 'just in case' measures when the risks don't justify them is damaging to the organisation and displace resources from other more pressing tasks.

Practical Steps to Prevent Abundance of Caution Behaviour

Many threats are generated by attackers and the solution is to counter them with security measures. On the other hand, the abundance of caution threat is voluntary – it is generated by the industry (regulators and operators) and there are practical steps that can be taken to eliminate it.

The more certainty the organisation has about its security performance and resilience, the more able it is to make informed judgements about threat and risk. In such an organisation, management understands the risks their organisation faces and has confidence in the measures in place to mitigate them. The best of these organisations have also established a no-blame culture which reduces disproportionate responses to threats and other dynamic security events, since executives, managers and staff no longer feel compelled to 'cover their backs' and are comfortable taking a measured response.

> "…deploying 'just in case' measures when the risks don't justify them is damaging to the organisation and displace resources from other more pressing tasks…"

Much good work has been done by the UK's Centre for the Protection of the National Infrastructure on Deterrence Communications1. Simply put, this is messaging intended to cause concern to hostile individuals about being detected. Deterrence communications is being used to good effect and promotes the message that security is strong and employees are engaged and vigilant, knowing the role they have in ensuring that security is kept that way. The trend towards an abundance of caution flies in the face of this and does the complete opposite, signalling security weakness and uncertainty.

2. Threat Assessment Training

The need for trained and experienced threat assessors and risk managers cannot be overstated.

3. Tried and Tested Security Management Methods

Proven methods exist for organisations seeking to gain certainty, assurance and peace of mind, and to be able make proportionate response decisions. Robust threat assessment processes coupled with outputs from three-dimensional security management will enable informed judgements to be made about threat and risk, particularly in response to dynamic situations. The reason we talk in terms of three dimensions of assurance is because it stresses the need for a holistic all-round view of the risks. This can only be achieved by understanding the threats, implementing appropriate mitigations and measuring their effectiveness.

The resulting decisive action accompanied by clear messaging will instil confidence and signal that the organisation has faith in its people, processes and security systems. The value of this cultural shift in promoting the right responses from personnel should not be underestimated.

We have always found an excellent place to start is the UK CAA's SeMS

Conclusion

In this age of uncertainty, dynamic threats and security events will continue to be a way of life for the industry. How an organisation responds to them speaks volumes about their security certainty.

Organisations should be under no illusion: 'abundance of caution' approaches are damaging, can compromise its deterrence communications and send out undesirable signals to the public and media. Yet this invisible threat could be brought under the organisation's control if it was enlightened enough to recognise the issue and adopt the proven techniques.

The goal is to achieve three-dimensional assurance by understanding the threats, implementing appropriate mitigations and measuring their effectiveness. Abundance of caution has no place in a mature security system.

Andy Blackwell is the former Head of Security of Virgin Atlantic and now a Managing Partner of 3DAssurance, a threat and risk management consultancy.

1. For further information about Deterrence Messaging see https://www.cpni.gov.uk/deterrence
2. CAA UK SeMS Framework:
https://publicapps.caa.co.uk/docs/33/CAP%201223%20SeMS%20Framework_Feb18

RELATED ARTICLES - MORE FEATURES