TERROR'S TIMELY REMINDERS

Aviation security experts Andy Blackwell and John Wood assess the aviation sector's response to an ever-changing terror threat

If your Chief Executive asks "What's the chance of an attack happening here?" - what would your answer be?

Two recent incidents serve as a reminder of the unhealthy interest terrorists retain in civil aviation; firstly, Al Qaeda's (AQ) latest call to action made specific mention of targeting the US by aircraft using new techniques and tactics.

More recently, the mortar attack against a commercial helicopter providing transport support to a UN humanitarian mission in Somalia, by AQ affiliate, Al Shabaab. Whilst some may have forgotten about AQ, they haven't forgotten about aviation.

Worse, it's not just terrorists that those responsible for managing threats and risks must contend with. Aviation is exploited by organised crime groups trafficking of humans, drugs, and weapons. All this at a time when the sector is recovering from the impacts of the pandemic.

Whilst many organisations point out safety and security are top priorities, this statement is most frequently issued after a significant breach.

The business view

The business view is that security is one of those necessary evils whose costs need to be kept under control. Meanwhile the Security Department is doing its best to achieve compliance with regulations and procedures in the hope that this makes the business secure.

Both viewpoints are wrong and a new way of thinking is needed on both sides if we are to build agile defences.

Focusing on cost control opens the business to crime and

> "WORSE, IT'S NOT JUST TERRORISTS THAT THOSE RESPONSIBLE FOR MANAGING THREATS AND RISKS MUST CONTEND WITH."

terrorism; It's not mandatory to lock your front door when you leave home, but it is a wise precaution.

When a business focuses solely on cost control, it is very hard for the Security Department to get approval for wise precautions that are not mandatory.

In many cases, security managers don't have the business know-how to explain security issues in terms directors can grasp.

So, they press on with a patchwork of the tools and resources they can afford, rather than what they really need. They know there are unmitigated risks, they try all kinds of approaches but still carry the stress and fear of 'the big one'.

Conversely, the directors assume that being compliant with the security regulations is enough protection for the business, and perhaps more importantly, their backsides.

However, terrorists and criminals are inventive and find new ways to harm us, so unless a business tries to anticipate their inventions, it is leaving the door open to new attacks.

Trust in the regulations may actually be the biggest obstacle to closing that door properly. A kind of institutional complacency is born out of three commonly-held fantasies: Wood said "compliance with regulations is enough to keep us safe", "inspectors will tell us if we're not compliant" and "in any case, what's the chance of that happening here".

Too often this 'reliance on compliance' means the risk management process becomes a chore with little chance of matching the agility of the enemy or identifying their new threats.

It's the same with security procedure manuals. Like regulations, procedures are slow to respond to threats that are constantly evolving and can create similar institutional complacency. The Inquiry into the Manchester Arena Bomb after the Ariana Grande concert in 2017 concluded:

"[The] specific risk assessment for the concert was inadequate: it did not identify the threat from terrorism as a potential hazard and had descended into a box ticking exercise".

If procedures and regulations don't keep you secure, what does? Thankfully, a terrorist attack is an infrequent event, but the underlying vulnerability is not: the Security Department going through the motions but not really thinking hard about it. Businesses not trying to understand what the threats are or acknowledge new ones, refusing the Security Department the budget for a strong response to a new big risk.

To make a business truly secure, the single most effective step is to set up Threat and Risk Management involving security and business managers, delivering products of substantial thought and effort. It's one small step for the Security Department but a giant leap for security.

The business needs to take a step forward too. Instead of treating it as a cost to be controlled, the business must manage the Security Department as a risk-management service. Security risks are business risks, requiring business managers to take an active part in the revitalised Threat and Risk Management 'system'. It's one small step for the business but another giant leap for security.

If only these two small steps were possible, if only it were possible to bring the business and the Security Department together to fight the common enemy.

This is not as difficult as you might think. It can be built on proven mechanisms used already in every business and does not need to be a big budget project. It can incrementally replace pieces of the patchwork to create a coherent comprehensive 'system' – no mishaps, no gaps, no overlaps.

The system would also make the business compliant with regulations organically, as a byproduct of being secure not an end in itself.

Driving security levels

The two small steps would create the forum for the security team to engage with the business in jointly managing risks would start to drive security levels upwards. They would consolidate the company's existing Risk Management procedures which would further improve security levels and certainty.

Finally, they would lead to upgraded governance controls to ensure the procedures continue to operate effectively. The key to this is a robust threat and risk process that is relentless in searching out and understanding the risks to the business before deciding how much to invest in mitigation, making this a business decision not the security department going cap in hand with bad news to beg for more budget.

The design of that process will naturally lead to management commitment and evolution of a security-aware culture through the organisation, together with mechanisms to keep the threat and risk process up to scratch. Organisations do it routinely for finance, brand protection, and health and safety: it is no harder to do it for security. ■

Andy Blackwell

Blackwell was formerly Head of Corporate Security with Virgin Atlantic, responsible for all aspects of the airline's security activities. He was heavily involved in the responses to several major terrorist attacks and disruptive events against aviation. The Metropolitan Police Service has commended Blackwell for demonstrating a high degree of professionalism and providing an exceptional level of service.

John Wood

Wood is a Security Management Systems (SeMS) subject matter expert, previously responsible at the UK CAA for formulating the SeMS strategy and developing the framework with industry partners. He is now a director of 3DAssurance, specialising in risk and security management. Wood is experienced in the design and implementation of effective strategic change in public and private sectors.