Sep 10, 2021 14:22 BST

# Formation flying: spotlight on aviation security

The aviation sector's threat landscape is complex and dynamic. Terrorists and other malicious actors retain their unhealthy interest in civil aviation, but it is not only conventional physical attack methods the sector has to concern itself with. Increased levels of digitalisation are attracting persistent attention from cyber criminals too, as they try to exploit the valuable personal and corporate data within the industry.

With more aviation operations moving online, combined with the current siloed working nature of the sector, organisations face an increased cyber threat.

Aviation security has traditionally been a specialised function with specific tasks largely driven by regulatory requirements. This has tended to obscure two self-evident and increasingly significant issues.

- First, the true purpose of security is not compliance with regulatory requirements, but protection of the business and its stakeholders from harm caused by malicious actions. Regulation inevitably lags behind the latest innovations in security threats, and organisations need to address new risks as soon as they emerge.
- Secondly, cyber security is fundamental to safe and secure aviation. With the increasing digitalisation of all aspects of aviation operations, from ticketing and inflight entertainment to avionics and air traffic management, aviation security teams are aware of the rising threats of cyber attack but can lack the skills or resources to identify or manage them. While many recognise the importance of collaboration between the physical and cyber security teams, organisational structures and governance arrangements often create obstacles to effective cross-departmental working.

Responsibility for managing risks to business, operational and control systems is dispersed across IT security, aviation security and flight safety. But the dynamic nature of cyber threats creates more attack opportunities than many realise – particularly for hybrid attacks, where a cyber attack facilitates a physical/kinetic breach, or vice versa. This increases the risk of warning signals being misinterpreted or missed altogether.

A further major concern is the growth in cyber-based insider threats: the risk of accidental or deliberate disruption by individuals with legitimate access is greatly magnified by the interworking of cyber and physical systems and the potential for hybrid attacks.

Operators can enhance their aviation security defences by taking three actions based on proven techniques and frameworks that can be adopted incrementally without disrupting the business.

- **Create the conditions to facilitate collaboration**. Within existing governance arrangements, the objectives and budgets of security teams should be adjusted to demand and facilitate collaboration.

- **Drive the evolution of collaborative security methods.** Operating models should be interwoven with communication and collaboration processes to manage risk at a high level without compromising each team's detailed techniques and skills.
- **Redouble efforts to manage the people risks.** The organisation's approach to insider threats should be enhanced to include the identification, risk assessment and treatment of insider threats with the 'mainstream' aviation security risks and risk management. This will require groups not normally considered to be security-focused, such as HR, legal and risk management to take a more active role in securing the organisation.

Lawrence Baker, aerospace technical lead at NCC Group, said: "Aviation organisations need to evolve their current approaches to safety and security to adapt to the rapidly evolving threat landscape that the sector faces in this time of rapid digitalisation.

"By adopting a collaborative and proactive risk-based approach, the sector will be able to keep pace with cyber threats and effectively exploit the benefits of digitalisation. The frameworks and methodologies for achieving this are already available – what is needed now is an openness to collaboration and change."

Andy Blackwell, consultancy practice director at 3DAssurance, said:"Terrorists and other bad actors continue to plan attacks on aviation, and hybrid threats give them new options, including greater exploitation of insiders. As connectivity and digitalisation increase, the cyber threat continues to grow and we need a new kind of vigilance and a new way of working."

To delve deeper into the subject, check out the NCC Group and 3DAssurance whitepaper which offers insights into the current cyber security risk in the aviation sector and makes recommendations for a toolkit of comprehensive security governance and management.

Download the full whitepaper [here](#).

**NCC Group – securing our connected future**

Society and industry's ever-growing reliance on technology has been

exacerbated by exponential digital transformation. Software and cloud consumption, driven by the Internet of Things (IoT), has never been higher, and the digital supply chains upon which our connected environment depends have never been more complex and interdependent. And as the fall-out from ransomware attacks and technical outages alike has shown, we have never relied more on the smooth functioning of digital technologies than we do now.

As society and industry's dependence on the connected environment and the associated technologies increase, we use our global insights to help organisations assess, manage, and develop their cyber resilience posture, enabling them to confidently take advantage of the opportunities that sustain their business growth.

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

## Contacts

**NCC Group Press Office**
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

**NCC Group - Financial Media Enquiries**
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

**Regional Press Office - North America**
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750