TROUBLE AHEAD?

Lawrence Baker *navigates aerospace cyber turbulence amidst compliance burdens*

The aerospace sector has long been synonymous with engineering excellence and uncompromising safety standards. But as the industry starts to become ever more digital and interconnected, it now faces a new normal in which cyber security must command equal attention.

Aerospace has long been conscious of cyber risk through well-established, globally harmonised safety regulations. But true cyber resilience must extend into digital ecosystems and supply chains that sit outside traditional aerospace structures. With fewer existing frameworks and limited international alignment, the sector must evolve its approach at pace – especially as cyber criminals are increasingly targeting aerospace for ransomware's large financial gains. The disruption caused by such attacks can cascade rapidly across interconnected systems, suppliers and third parties, as seen in the September 2025 attack on Collins Aerospace. The failure of a single IT system triggered delays and operational chaos across multiple airports. There are three key trends shaping what cyber risks the aerospace sector is facing, and how they should respond to them.

With geopolitical tensions rising, Governments are treating cyber threats with the same level of urgency and strategic importance as traditional military threats. Now that cyber security is an integral part of national defence, critical sectors like aerospace are experiencing the rapid development of strict laws, mandatory reporting and tighter oversight. Private aerospace companies face the mounting pressure of being considered an extension of national security infrastructure – with requirements of implementing stronger cyber defences, building fortified supply chains and fool-proof incident response plans on their to-do list.

After an intense period of policy discussion, clearer regulation is on the horizon. Governments are now consolidating regulations so organisations can better navigate requirements. The UK has built on its Security of Network & Information Systems (NIS) Regulations with the Cyber Security and Resilience Bill, to reduce the compliance burdens which critical industries like aerospace faces. But expectations for organisations to meet regulations are rising in line with regulators' abilities to enforce rules, prompting the aerospace sector to get on top of requirements sooner.

Aerospace's vital nature to the UK's infrastructure means it needs to get on top of its compliance requirements

Incident reporting has become increasingly complex. But initiatives like Australia's Single Reporting Portal, a centralised platform which guides organisations through the reporting process, simplifies the task for aerospace and other critical industries. This signals that in the future, aerospace organisations will need fewer compliance and legal resources to unpick cross-regulation complexities. However, investment in long-term, strategic cyber security programmes will still be integral.

Threats are rapidly evolving, from physical security to AI-enhanced vishing and aerospace's elevated profile means it's high up on target lists. As the attacks on Collins Aerospace in September 2025 proved, the interconnected nature of aerospace and its reliance on a multitude of suppliers and third-party facilities, means there's no such thing as an isolated threat. In Q3 2025, Industrials accounted for 30 percent of cyber attacks, signalling the value it holds to attackers.

The shifting objective behind attacks is also putting aerospace companies in the spotlight. Nation-state attacks are growing more prolific and, as their objective is often to cause mass disruption, they focus their efforts on targeting critical national infrastructure (CNI) and essential services. Aerospace's vital nature to the UK's infrastructure means it needs to get on top of its compliance requirements.

Aerospace's dual role in CNI through essential transportation, as well as in national defence, puts it in a unique position where its exposure to cyber criminals is two-fold. With cyber adversaries growing more sophisticated by the day, aerospace organisations must evolve to keep pace. They need to reinforce internal resilience across aircraft, satellites and ground systems and safeguard the complex, interconnected supply chains that sustain the sector.

Governments have varied in their speed and transparency levels around regulation, leading to policy which overlaps, conflicts with each other and complicates compliance, risk assessments and investments. Some critical infrastructure cyber regulation has ended up being passed around governments, delaying compliance. Regardless, there is a web of regulation helping the aerospace sector accelerate its preparedness rapidly.

It's essential to reiterate that the pressure cyber criminals are putting on aerospace companies is far from a fleeting trend. While attackers have been known to move their focus from sector to sector, such as Scattered Spider's move from targeting UK retailers to US aerospace – cyber security is not a temporary agenda point. The disruption it can cause means that it will always be a high-profile target for nation-state attackers.

In response to escalating cyber risks, governments are deploying regulation at unprecedented speed – placing aerospace under sharper scrutiny than ever before. While the volume of new rules can feel daunting, each targets a vulnerability amplified by recent incidents.

In the UK, the Cyber Security and Resilience Bill will strengthen incident reporting requirements and gives the Government greater oversight of supply chain cyber risk. This acknowledges that aerospace resilience depends on more than the defences of individual organisations. Across Europe, NIS2 and the Cyber Resilience Act raise the minimum security bar across the EU and for any company supplying into it, driving a shift from checkbox compliance to more strategic, long-term investment.

The European Union Aviation Safety Agency's (EASA) Part-IS introduces an information security management system aligned to aviation safety requirements. This ensures operators, manufacturers and maintenance organisations embed cyber protections into core safety processes. By aligning with broader international frameworks led by the International Civil Aviation Organisation, Federal Aviation Administration, EUROCAE, RTCA, and SAE, the sector is shaping a more consistent global baseline for aviation cyber protection.

The EU AI Act adds a new layer of responsibility for organisations deploying AI in aircraft systems, ground operations or air traffic environments. AI is becoming central to aviation efficiency, yet its vulnerabilities, from data poisoning to model manipulation, require careful governance. The Act's classification of many aerospace use cases as 'high risk' reflects this dual role of AI as both an innovation driver and potential entry point for attackers.

THOSE THAT INVEST IN RESILIENCE NOW WILL BE BEST POSITIONED TO PROTECT CUSTOMERS

These regulations land during a period of sector-wide turbulence of resource pressures, supply chain instability and tightening budgets, but the regulations objective is clear. They are designed to standardise expectations, strengthen weak spots and give regulators better visibility. The key challenge for aerospace organisations will be balancing speed with accuracy, as regulators now expect coordinated, near-real-time reporting even when information is incomplete or distributed across multiple business units.

The aerospace supply chain is vast, interconnected and spans international borders. It's also highly vulnerable. The Collins Aerospace incident underscored a simple truth: aerospace is only as strong as its weakest vendor. Resilience-by-design practices must become the default for all OEMs, to embed security into design and manufacturing processes to give products the greatest protection from day one.

Organisations should build trust with all third parties to foster collaboration and shared responsibility for resilience. Using a zero trust approach will ensure organisations are technically enforcing and verifying trust in the security of their systems on a continuous basis.

Equally critical is improving visibility across IT and operational technology (OT) environments. As aircraft systems, airports and flight operations become more digitally intertwined, the boundary between OT and IT becomes increasingly blurred. A larger attack surface means attackers can move between domains undetected.

This is not a one-off exercise. Supply chains are in constant movement and require continuous monitoring, regular engagement with suppliers and shared threat intelligence to keep pace with attackers who often target third parties first.

Beyond traditional IT threats, new operational domains mean new risks. AI regulation, particularly under the EU AI Act, is reshaping how aerospace develops predictive tools, diagnostics and autonomous

functions. Both EASA and the UK Civil Aviation Authority have outlined the proactive steps they are taking to ensure the responsible use of AI in the sector, such as increasing internal skills and evaluating worldwide best practices. AI systems hold enormous promise for improving efficiency and safety in aviation, but they must be governed properly. Without robust guardrails, AI models can be compromised, manipulated or used to automate attacks at scale.

THE AEROSPACE SUPPLY CHAIN IS VAST, INTERCONNECTED AND SPANS MULTIPLE BORDERS

Likewise, new technologies are being adopted as drone operations and advanced air mobility grow more capable, increasing the attack surface and risk of cyber threats. These developments signal a new era in which cyber security becomes inseparable from aerospace innovation. Those who treat security as an enabler rather than a constraint, will be best positioned to harness the transformative potential of these technologies.

To navigate tightening regulation and evolving threats, aerospace leaders should focus on the following five core priorities:

Stay informed. Cyber security regulatory monitoring must become a core CISO and executive function. With changes happening at pace, organisations must have dedicated capability to interpret, prioritise and prepare for new rules across every jurisdiction in which they operate.

Develop integrated strategies. Cyber and safety are intertwined. They are two sides of the same coin. Organisations need integrated strategies that encompass aircraft systems, ground operations, supply chains and emerging technologies.

Engage in collaboration. Aerospace ecosystems thrive on global cooperation. Leading organisations share intelligence in industry working groups, collaborate with regulators and peers on emerging standards, and work closely with legal to better negotiate security terms with major suppliers. Where appropriate, joint purchasing can also help negotiate stronger security commitments from major vendors.

Invest in training. People remain both the strongest defence and the most common vulnerability. Existing aerospace initiatives should be leveraged to include cyber security alongside their already strong safety cultures, to reach employees at every level so they can respond with confidence.

Test and refine incident response. Given growing expectations for rapid reporting, organisations must run frequent simulations and drills. Cross-functional teams, from engineering to legal, need to be able to respond rapidly and cohesively.

Cyber security is no longer a secondary consideration for the aerospace sector; it has become central to resilience, safety and national security. With regulations tightening and threats growing more sophisticated, the need for decisive action has never been clearer. Aerospace leaders must secure internal systems, reinforce supply chains and adapt to the demands of faster, more coordinated incident reporting.

Those that invest in resilience now will be best positioned to protect customers, maintain operational integrity and meet rising regulatory expectations. In an industry defined by precision and trust, cyber security is not just another obligation. It is the foundation that will keep aerospace airborne in an increasingly hostile and uncertain digital landscape ●

Lawrence Baker
is Global Aerospace Technical Lead at cyber security firm NCC Group.

AI is becoming central to aviation efficiency, yet its vulnerabilities require careful governance

Picture credit: Crown Copyright