Aviation MRO Under Siege: How the Industry Is Defending Against Rising Cyber Threats

As cyberattacks on aviation MRO increase, the industry's highly interconnected systems make it a prime target for ransomware and AI-driven social engineering.

Lina Vaskelė, Chief Risk and Security Officer at FL Technics

WA, UNITED STATES, April 8, 2026 /EINPresswire.com/ -- Cybersecurity is becoming an increasingly important issue for both individuals and businesses. It is estimated that, on average, global organizations face nearly two thousand cyberattacks each week. Last year, the costs to businesses totaled $10.5 trillion, and this figure is projected to reach $15.63 trillion by 2029. Cyberattacks impact nearly every industry, including aviation. According to Thales' report, the number of such threats increased by 600% between 2024 and 2025. With ransomware attackers targeting aircraft MRO as a primary focus, companies are stepping up and investing heavily in their cybersecurity tools.

Attempts to investigate and control the IT infrastructure of aircraft MRO companies are on the rise. Unsurprisingly, the global aviation cybersecurity market grew to $11.3B in 2025 and is projected to reach $29.4B by 2034, with an annual growth rate of 11.2%.

Aviation maintenance organizations are especially appealing to malicious actors due to the high level of operational decision-making and process complexity. By breaking into their security systems, attackers threaten to stop critical processes and disrupt the entire operations chain. The frequency of such attacks is further driven by AI-based social engineering, as reported AI-enabled cyber attacks increased by 47% worldwide in 2025.

“In aviation MRO, all systems are deeply interconnected. Various maintenance records, airworthiness data, supply chains, and operational schedules all influence each other. A single

cyberattack doesn't just target a single isolated point; it can spread throughout the entire infrastructure. If one part of the system fails, the risk quickly spreads to related processes and can cause consequences far beyond the initial target of the attack," says Lina Vaskelė, Chief Risk and Security Officer at FL Technics, a global independent aircraft MRO service provider.

With ransomware attackers targeting aircraft MRO as a primary focus, companies are stepping up and investing heavily in their cybersecurity tools

The road to unified cybersecurity policy

The international aircraft MRO community is working to establish consistent minimum standards across the industry. This is a crucial step for an industry that has historically had wide variation in cybersecurity maturity and has never implemented a unified cybersecurity policy.

> As digitalization progresses, the impact of IT systems on aviation MRO safety is becoming too significant to be viewed solely as a technological concern."
>
> *Lina Vaskelė, Chief Risk and Security Officer at FL Technics*

In 2024, the Federal Aviation Administration (FAA) issued a Notice of Proposed Rulemaking outlining required cybersecurity measures for aircraft, engines, and propellers. Similar initiatives are being undertaken in Europe as well. In February, the EASA directive Part-IS took effect, requiring organizations not only to have documented policies but also to demonstrate their effective implementation and readiness for oversight.

There are also international efforts. The governing body of the International Civil Aviation Organization (ICAO) has recently updated its Cybersecurity Action Plan, which urges member states to incorporate cyber risk management into their safety oversight frameworks.

"Such a unified regulatory step was unavoidable. As digitalization progresses, the impact of IT systems on aviation MRO safety is becoming too significant to be viewed solely as a technological concern. The industry has had to recognize that the line between the digital and physical realms, between software vulnerabilities and flight safety risks, has effectively vanished," says Ms. Vaskelė

She notes that the most common cyber risks come from gaps in identity management systems,

insecure external digital tools, and the human factor. In recent years, FL Technics has invested in various security measures, focusing mainly on strengthening protections, deploying advanced detection and monitoring systems, and enhancing access control and incident management. The main aim is to create multi-layered protection where human vigilance and technological controls work together as an integrated, complementary system.

“Employee training is undoubtedly the most important aspect. You can have the most advanced security tools, multi-layered protection, and state-of-the-art detection systems, but the truth is that the final decision always rests with a human. That is why personal awareness remains the very first and most crucial line of cyber defense,” says Ms. Vaskelė.

— END —

About FL Technics

FL Technics is a global provider of aircraft maintenance, repair, and overhaul (MRO) services. The company specializes in base and line maintenance, spare parts and component support, engine, APU, and landing gear management, full aircraft engineering, technical training, and aerospace logistics solutions. Certified under EASA Part-145, Part-CAMO, Part-147, Part-21, and FAA-145, FL Technics operates facilities in Lithuania, Indonesia, the Middle East, and the United Kingdom, with line stations worldwide.

FL Technics is part of Avia Solutions Group, the world’s largest ACMI (Aircraft, Crew, Maintenance, and Insurance) provider, operating a fleet of 187 aircraft across 6 continents. The group also provides a range of aviation services: MRO (Maintenance, Repair, and Overhaul), pilot and crew training, ground handling, and other associated aviation services. Supported by 14,000 highly skilled aviation professionals, the group is the parent company of over 250 subsidiaries.

Alge Ramanauskiene
UAB Particle Agency
email us here