Cybersecurity Fundamentals for Aviation

Safeguarding Your Aircraft

INTRODUCTION

Cyber threats are on the rise. Are you Protected?

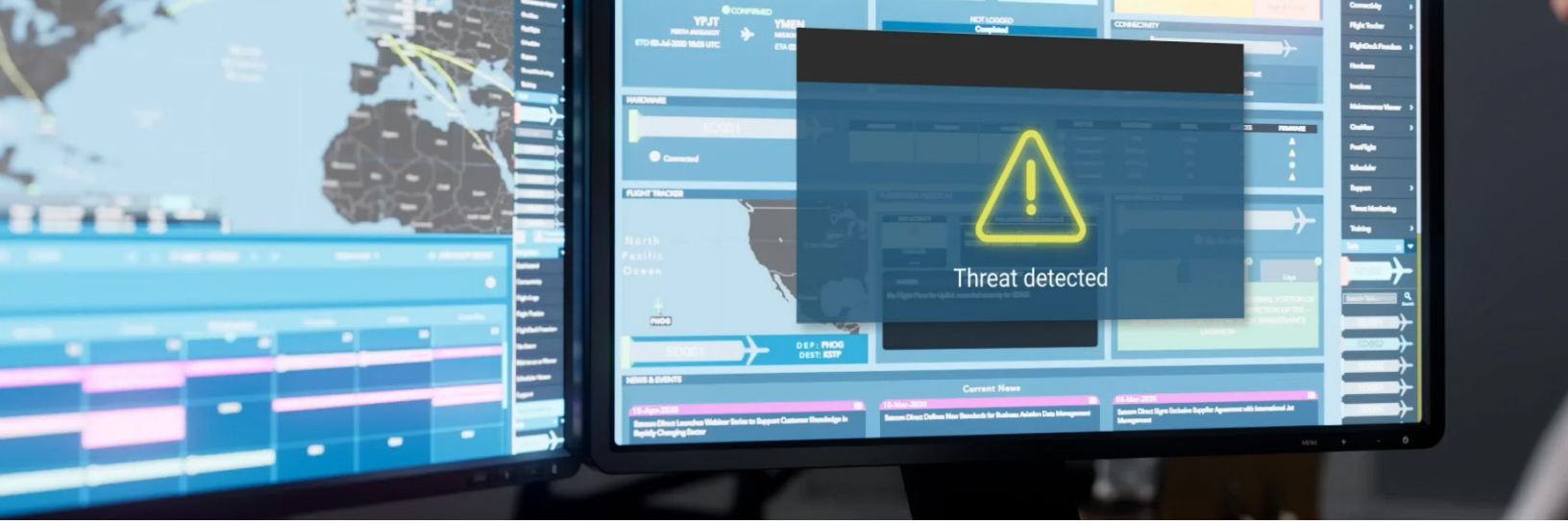
As technology continues to advance, passengers now expect the same level of digital connectivity in the air as they enjoy on the ground. Today's aircraft are equipped to support high-speed data transfer, allowing travelers to participate in video calls, stream, work remotely, and stay connected throughout their journey. Enhanced connectivity also empowers flight crews, improving operational awareness and elevating the passenger experience.

Yet, this surge in connectivity introduces significant cybersecurity risks. In 2023, billions of data records were compromised globally, with cyberattacks costing organizations millions and often remaining undetected for months. For aviation, the implications are especially serious: without effective cybersecurity measures, aircraft networks and passenger data are as exposed as they would be on any unsecured public network. As onboard connectivity becomes indispensable, protecting sensitive information at altitude is more urgent than ever.

STRENGTHENING DATA SECURITY: CYBERSECURITY STRATEGIES AND RISK MITIGATION

Cybersecurity is essential for protecting data transmitted between aircraft and organizational networks from unauthorized access and theft. Gogo is an industry leader in cybersecurity protection and addresses these challenges with advanced network security, continuous monitoring, and dedicated security operations centers to safeguard both air-to-ground and satellite communications.

A strong cyber defense strategy depends on ongoing education and vigilance among staff, suppliers, and passengers. Gogo prioritizes regular training, risk assessments, and the integration of robust security protocols into daily operations. By combining advanced technology with proactive monitoring and comprehensive training, charter operators and flight departments can effectively mitigate risks and protect passengers' critical data.



HIDDEN RISKS: HOW YOU MAY BE ENABLING CYBERATTACKS

Many people unknowingly increase their risk of cyberattacks by connecting to unsecured Wi-Fi in public places or by using thumb drives without knowing their source or ensuring they are password protected. These actions can allow malware or viruses to be downloaded onto devices, often without the user realizing it.

Additionally, failing to scrutinize unusual emails or clicking on unknown attachments can make users vulnerable to cyber threats. Sharing sensitive data with third-party suppliers also poses risks if those companies lack strong cybersecurity protocols, as valuable information can be exposed if their systems are not secure.

The best offense is a good defense. We recommend aircraft owners and operators, stakeholders, and suppliers be cyber vigilant and employ various tools to mitigate the threat. A combination of human understanding, implementation of tech protocols and investment in robust cyber management solutions can help protect aviation assets. Here's what you can do as a passenger to mitigate cyber threats:

Use passwords to protect the cabin Wi-Fi. We know flight departments can be reluctant to create Wi-Fi passwords due to the perceived inconvenience to passengers, yet the inconvenience far outweighs the potential risks. QR codes are a simple way to share the password.

Beware of phishing attempts, which often arrive as emails that look legitimate but are designed to steal sensitive information or install malware. Always be cautious with unexpected emails-especially those with urgent requests, unfamiliar links, or attachments-and verify the sender before clicking or responding.

When you travel, use a virtual private network. This creates another layer of defense when logging on to a hotel, restaurant or FBO network. Equally, when travelling to a new country, ask the IT department to confirm if it is high risk in terms of cyber events and if it is, leave data-rich devices at home and use loaner devices.

Minimize sharing data with third-party suppliers and confirm third-party suppliers' cyber protocols. Passenger manifests, for example, contain rich data, but if the catering company/ground transport company does not have cyber protocols in place, the data becomes vulnerable.

EMERGING TECHNOLOGIES SHAPING AVIATION CYBERSECURITY

Emerging technologies like AI and blockchain are rapidly reshaping aviation cybersecurity. While AI drives innovation and operational efficiency, it is also exploited by threat actors to launch increasingly sophisticated attacks. Generative AI can produce convincing phishing emails and realistic voice scams, while attackers use AI to cross-reference flight data, create deepfake impersonations, and automate large-scale attacks on inflight systems. Advanced AI also enables the development of undetectable malware, exploitation of system vulnerabilities, and more effective password cracking. The growing prevalence of nation-state-sponsored attacks and the evolution of malware into complex threats like ransomware and APTs underscore the high-stakes and ever-changing nature of cybersecurity in aviation.

However, for every new threat, there are equally advanced defensive measures. AI-powered cyber defense tools can detect threats early, analyze behavioral anomalies in flight data and network traffic, and trigger rapid responses to incidents. When combined with human expertise and robust protocols, these technologies form a powerful defense against evolving cyber risks. As the sector continues to evolve in response to increasingly sophisticated attacks, aircraft owners and operators, stakeholders, and suppliers must remain vigilant-adopting layered security strategies, investing in advanced solutions, and prioritizing ongoing education to safeguard critical assets and operations in this ever-changing digital environment.

GOGO CYBERSECURITY SOLUTION OFFERS:

Layered Defense - We understand the unique cybersecurity challenges faced by the business aviation/milgov industry. Our solutions are customized to meet your needs.

Proprietary Threat Detection - Stay one step ahead of cyber criminals with our state-of-the-art threat monitoring and risk mitigation. Our algorithms continuously monitor your inflight systems, identifying and neutralizing potential breaches before they can disrupt your operations.

Secure Data Transmission - Fly with confidence. Our encryption protocols ensure end-to-end security for your inflight communications, protecting your sensitive data from interception or unauthorized access.

Real-time Monitoring - We maintain constant vigilance over your inflight network, monitoring for any suspicious activities. Our dedicated team of experts are on standby 24/7 to respond swiftly to any emerging threats, ensuring the uninterrupted safety of your digital environment.

Compliance and Certification - We adhere to industry regulations and best practices. Our cybersecurity solutions are developed in compliance with industry standards, giving you peace of mind knowing that you're operating within a secure and compliant framework.

GOGO PROVIDES THREE CLEAR LEVELS OF SERVICE TO SUPPORT CYBERSECURITY MITIGATION

Threat Monitoring: The entry-level service provides active threat monitoring by proactively observing live flight data behavior. Human experts work with AI and refined machine reading technology at our NOC to evaluate data transmission. If the system notes discrepancies, remedial activity follows.

Advanced Encryption: Purpose-built for business aviation, this service uses our router platforms and infrastructure to apply proprietary technology to optimize a secure, accelerated tunnel through which encrypted, anonymized data passes from the aircraft to the ground and back. The system effectively protects the entire aircraft network.

Private Network: Transforms the aircraft cabin into a secure corporate workspace. The data never touches the public internet, effectively making the aircraft as secure as an office while also giving visibility into the network for threat monitoring.

Gogo's Cybersecurity Dashboard available in the SD Pro app

GOGO'S PORTFOLIO OF TRAINING OPTIONS

Gogo is a strong advocate for training and education of inflight connectivity and cyber defense. We run cyber awareness courses that are constantly updated for aviation IT professionals, crew, and passengers. Our Aviation CyberThreat Awareness course is designed specifically for business aviation professionals, owners, and operators. The program navigates the complexities of security and cyber threat prevention from an aviation perspective. It identifies common risks, defines attack methodology, and describes current cybersecurity concerns within aviation to raise awareness about inherent vulnerabilities. Modules relating to data protection during international travel are complemented by information pertaining to the use of personal digital devices before, during and after a flight. This human element is a vital foundation on which to build out cyber vigilance.

CONCLUSION

Inflight connectivity is becoming an integral part of modern aviation; the industry faces a rapidly evolving landscape of cyber threats that demand proactive and comprehensive defense strategies. Gogo's layered approach – combining advanced technology, continuous monitoring, and dedicated training-demonstrates how aviation stakeholders can effectively protect sensitive data and maintain operational integrity at altitude. By adopting robust cybersecurity protocols, investing in ongoing education, and remaining vigilant against emerging risks, aircraft owners, operators, and partners can ensure the safety and resilience of their digital environments. As cyber threats continue to grow in sophistication, a commitment to best practices and adaptive solutions remains essential for safeguarding the future of connected aviation.