Cybersecurity in the business aviation industry

Cybersecurity isn’t a product we sell – it’s what we do.

Rockwell Collins
Building trust every day
Introduction

If cybersecurity is treated as a product, that means it’s inherently something bolted on and not network engineered from the very beginning. We provide connectivity for customers throughout the entire aviation ecosystem, from hundreds of airlines and airports to more than 4,000 business jets. It’s our number one responsibility to make sure information gets from A to B reliably, efficiently and cost effectively. Most critically it’s our job to ensure your data arrives at its destination securely. Without data security those other things lose more than a bit of their punch. Cybersecurity cannot be an upsell. It can’t just be built onto the foundation of our network, it has to be the foundation.

At Rockwell Collins, we operate on the principle of hypervigilance. Our network is built to constantly analyze and identify normal and suspicious activities. We monitor data flow and touch points 24/7/365 from our network operations center. As a connectivity provider and systems integrator, our customers’ trust is everything to us, and it’s why we dedicate a team of experts solely to cybersecurity.

No unsolicited traffic goes into an aircraft with our ARINCDirect SM cabin connectivity without permission. We know all the traffic crossing our network, including applications, users, content and devices. We mask aircraft IP addresses with our public one so yours cannot be accessed and we utilize the most secure Wi-Fi standard available today, the same one commercial airlines use to protect credit card information. Passengers can do everything they want – email, video chat, text, watch a movie, use social media, surf the internet – assured of the security of these services while they’re in flight.
Our ARINCDirect\textsuperscript{SM} threat monitoring detects anomalies that could lead to an attack

There are various levels of risk associated with data security depending on the access point in the chain of connectivity. Some – Rockwell Collins’ network, Inmarsat’s network, the IPsec tunnel for example – are very low risk. Security admin access to cabin router configuration is slightly higher. Others like onboard devices and public internet traffic beyond our ground network are considered the highest level of risk.

Rockwell Collins utilizes threat analytics as the backbone of our cybersecurity practice. Our first line of defense is a strong firewall to prevent modern threats by scanning and addressing vulnerabilities. With analytics engineered into our network to learn and identify normal and suspicious activities, we are able to manage the whole ecosystem. Our firewall prevents any unwanted traffic or unsolicited connection up to the aircraft by keeping track of the data going out. If there is no matching outbound connection, the firewall will prevent an inbound connection to the aircraft. Our network will block any device that it does not recognize and is not registered on our gateway.
Cybersecurity throughout the lifecycle

We consider security part of the full product lifecycle. Our security team works closely with our product development team to ensure that we provide safety communications and consultation that goes all the way back to the hardware. They are responsible for architecture and network analysis, SELinux policy analysis and design, embedded Windows® and Linux® OS hardening, as well as cryptographic design and implementation.

The security team works with all levels of customers to ensure that security capabilities are understood. Starting with Threat Analytics, the security team engages system developers to design and implement the right level of security. They provide consulting for security vulnerability and help identify weakness early.

This includes:

- Overall system security architect review
- Aircraft risk and threat assessment
- Threat modeling
- Penetration and fuzz testing
- Support throughout the certification process
- Secure software distribution
- Post entry-in-service: recurring assessments, log analysis, support for incident response, forensic analysis of compromise
Rockwell Collins sets high-security standards

Rockwell Collins’ ARINCDirect operates connectivity services from two primary co-location facilities in New York City and Slough, UK. The cybersecurity compliance standards are SOC 2 and ISO 27001.

SOC 2 is a standard designed for technology companies, including: data centers, IT managed services, SaaS vendors, cloud-computing-based businesses and other technology. SOC 2 criteria is based on the Trust Services Principles (TSP) of security, availability, processing integrity, confidentiality and privacy as well as controls outside of financial reporting.

ISO 27001 is an internationally recognized best practice framework that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). ISMS is a systematic approach to managing sensitive company information including people, processes and IT systems.

The PCI Security Standards Council offers comprehensive standards and supporting materials to enhance data security for payment cards. They include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents.
Cybersecurity starts with you

A crucial and often forgotten element of cybersecurity is educating passengers on how to take steps to protect their information themselves. There are multiple touchpoints in the chain of connectivity within passenger control to help ensure their data’s security. Awareness training that educates passengers on how to recognize potential situations that may compromise the data security in the aircraft, such as phishing email, downloading dangerous applications and easy to decrypt passwords, can go a long way on its own. In addition, you’ll want to ensure the software and hardware of all devices brought onboard have the most up-to-date anti-virus protection.

Precautions should always be taken when connecting anything to the public internet, including the aircraft itself. Many hangars are equipped with Wi-Fi hubs that allows for easy and free access to public internet. As with any equipment, precautions should also be taken when the aircraft is on the ground and connected to public internet for any purpose, and especially if it is to update any of the aircraft system.
Building trust every day.

Rockwell Collins delivers innovative aviation and high-integrity solutions that transform commercial and government customers’ futures worldwide. Backed by a global network of service and support, we are deeply committed to putting our solutions to work for you, whenever and wherever you need us. In this way, working together, we build trust. Every day.

For more information, contact:

Rockwell Collins
2551 Riva Road
Annapolis, MD 21401
866.633.6882 | +1.410.266.4000
ad-sales@rockwellcollins.com
rockwellcollins.com