How safe is your data in the cabin and cockpit?

CYBERSECURITY IN THE SKY

STORY BY LINDSEY MCFARREN

Cockpit connectivity has advanced considerably during the past decade, and Wi-Fi internet access in the cabin is now considered a standard requirement for most business aviation users. What vulnerabilities are created in the cabin and cockpit by the conveniences of always being connected? How do you mitigate those vulnerabilities to ensure your data and the cockpit are secure?

"Like any risk assessment, it is important to look at the issues throughout the operation," said Bob Richard, staff vice president for ARINCDirect flight support services at Rockwell Collins. "Taking a step back and working with experienced professionals in your company and your service providers allow you to examine each part of your flight operation and identify what risks may exist, how they might affect you and what you can do to mitigate them. Business aviation is very safe and secure, but it's important to regularly test and evaluate your systems with a view to implementing best cybersecurity practices. We all share in this responsibility across our industry."

Cabin connectivity

Everyone knows working with sensitive data over a public Wi-Fi connection is like taking out an ad in the newspaper publicizing your bank information or social security number. A low-level hacker with some basic skills can see and use your data for nefarious purposes.

Experts recommend using a VPN or other secure network even when using cabin Wi-Fi in a business aircraft, where passengers are likely to be associated in some way – that familiarity can create a false sense of security.

"It's true that on a business aircraft you would tend to know everyone, but do you trust every one of them?" asked Kelli Wolfe, principal systems security engineer at Rockwell Collins. "There are always risks involved in remote use anywhere, so it's important to use best practices and common sense."

Some on-aircraft networks are more secure than others. Although a network on a commercial airline is only as secure as a hotel or local coffee shop, a business aircraft's network that is part of the company's terrestrial network may be much more secure. It can function as part of the company's network. For example, Satcom Direct Private Network, the Rockwell Collins ARINCDirect network, and some other services allow you to operate on your company network so network security in the aircraft is the same as network security in your office.

Traditional cybersecurity practices are critical to securing your data while connecting in the aircraft. Maintaining control of your devices, avoiding charging devices in USB connections, and using strong passwords are all recommended methods of mitigating cybersecurity vulnerabilities in the cabin.

TRADITIONAL CYBERSECURITY PRACTICES ARE CRITICAL TO SECURING YOUR DATA WHILE CONNECTING IN THE AIRCRAFT. MAINTAINING CONTROL OF YOUR DEVICES, AVOIDING CHARGING DEVICES IN USB CONNECTIONS, AND USING STRONG PASSWORDS ARE ALL RECOMMENDED METHODS OF MITIGATING CYBERSECURITY VULNERABILITIES IN THE CABIN.

Cabin connectivity is a more vulnerable target than cockpit connectivity for potential hackers for one simple reason – familiarity with the technology.

"The internet access system for passengers in the cabin is a much more likely target than the cockpit and has more in common with current terrestrial networks than typical hackers are familiar with," said John Zban of Satcom Direct.

"It should be treated as part of the company's IT network in just the same way as if it was the CEO's office in the headquarters," Richard added.

Cockpit connectivity

How vulnerable is the cockpit to cyberattacks and hacking? Cockpit technology should be considered in two separate categories – installed, certificated hardware and portable electronic devices.

Some "e-enabled" aircraft are issued a special condition from the FAA. The special condition governs not only the design of the aircraft but the instructions for continued airworthiness and procedures for the operator to maintain security of the aircraft network for installed hardware. Several general aviation aircraft types have been issued a special condition, including some Learjet, Cessna and Gulfstream models, as well as the Embraer EMB-500.

Advisory Circular 119-1, Airworthiness and Operational Authorization of Aircraft Network Security Program, responded to technology changes in the cockpit. Previous aircraft designs used Aeronautical Radio Inc. or military standard data buses to connect flight-critical avionics systems. The introduction of certain technology advances, including Internet Protocol connectivity, presented new security challenges and required a new approach to cockpit data control.

The AC describes an acceptable means of obtaining operational authorization for an aircraft certified with a special condition related to security of the onboard security network and, although intended for Part 121, 125, 129, and 121/135 operators and the repair stations that work on these aircraft, the AC provides good guidance for all aircraft operators. For example, the AC recommends plans and procedures regarding training, event recognition and response, and controlling access to equipment.

Most information transmitted to the installed hardware in the cockpit – for example, through controller pilot data link communications and aircraft communications addressing and reporting system end systems – utilize encoded messages and certain allowable communications medium. They operate over private, controlled networks such as Rockwell Collins' ARINC Global Network and through proven operational procedures aimed at ensuring all parties agree to all messaged instructions.

While these two levels of security – encoded messages and specific allowable communications medium – are generally accepted by the industry and regulators, the real fail safe for cyberattacks are pilots.

"Malicious messages to the cockpit would not allow

Continued on following page

CYBERSECURITY IN THE SKY

Continued from page 33

anyone to exert control over aircraft systems as a crew member is required to accept, acknowledge and act upon CPDLC messages," Zban said.

The second category of cockpit connectivity comes through portable electronic devices. More and more pilots use portable electronic devices as electronic flight bags, typically using a common device – the iPad. The iPad and some other portable equipment are Class 1 EFBs. Use of these EFBs by Part 121, 125, 135, and 91 subpart F and subpart K operators must be authorized by the FAA, and their use is limited by AC 120-76A. However, the AC provides good guidance for all aircraft operators and pilots regarding general security measures.

It's always good to assume the worst in any safety-critical environment, so cabin devices must be, and are, segregated and protected from standard cabin connections. Certificated, installed hardware includes built-in protections, but portable electronic devices are vulnerable to attacks in the cabin system. An Ethernet router can be used to create a firewall between connectivity and the cockpit. Portable electronic devices used in the cockpit also should have current, reputable anti-virus/anti-malware software installed.

Train to mitigate cabin and cockpit vulnerabilities

Wolfe and Zban recommend training to mitigate cybersecurity vulnerabilities in the cabin and the cockpit. Both pilots in the cockpit and passengers in the cabin can benefit from cybersecurity training.

Flight departments and air carriers should provide their pilots with basic cybersecurity training, including using strong passwords, safe charging of devices, and properly logging out of devices. Pilots should be trained to verify messages inconsistent with expectations and standard operations by using voice communications.

"One of the primary reasons we have pilots in the cockpit is to use their human brains and apply critical thinking," Wolfe said.

Some aircraft operators – especially flight departments, which tend to have a clear nexus with their passengers – might consider offering passengers training or at least ensure passengers are aware of and comply with the company's security policies when on the company aircraft.

Passenger training should include the same best practices as those for pilots: basic cybersecurity awareness and strong password development, plus use of VPNs or other secure network access.

The increased vulnerability of the cabin system makes passenger awareness and training even more important.

Regulatory climate

The FAA and the International Civil Aviation Organization are looking closely at cybersecurity. An Aviation Rulemaking Advisory Council on Aircraft Systems Information Security/Protection recently presented the FAA with 30 recommendations for improving cybersecurity in the national airspace system.

The goal of the ARAC ASISP working group was to consider regulation, policy, and/or guidance to identify aircraft vulnerabilities and mitigate risks in a harmonized manner with other aviation authorities and regulators. It remains to be seen what will come of the 30 recommendations, many of which relate to certification or design, but some include agency or industry best practices in operations.

The ICAO also has taken on cybersecurity concerns through the AvSec panel, a group of industry and government security experts. The ICAO is focused on information sharing and coordination across civil aviation safety and security to address aviation cybersecurity on a global level. In addition, the ICAO Annex 17, Chapter 4 outlines preventive security measures.

For now, certificated, installed cockpit hardware in U.S.-registered aircraft is standardized through special conditions issued by the FAA, and portable electronic devices are standardized for commercial air carriers through the EFB authorization process. But cabin connectivity systems and portable electronic devices for Part 91 operators require industry-driven, voluntary compliance with best practices. Additional regulation, standards, and/or best practices are likely to be issued by national aviation authorities and the ICAO during the next several years to address the ever-changing environment of cyberrisks.

To keep your data secure, whether as a passenger in the cabin or pilot in the cockpit, in most cases, the basics of cybersecurity are most crucial: Be aware of the risk, use strong passwords, consider use of a VPN for passengers, and use effective anti-virus/anti-malware software on all devices.❑