PENTASTAR Aviation
SETTING THE STANDARD®

APRIL 2018

CYBERSECURITY

HOW BUSINESS AIRCRAFT AVOID THE RISKS

TABLE OF CONTENTS

INTRODUCTION

In recent years, cybersecurity has been a leading topic of discussion in the news with stories proving that even companies boasting the most elaborate security systems are at risk of hacking. It is happening in every industry, and as quickly as new measures are put into place to safeguard against these attacks, there are resourceful adversaries consistently searching for vulnerable areas within network resources, ready to strike again.

There has been much discussion recently regarding cybersecurity as it relates to airliners, general aviation, and business aviation. The latter is most relevant to Pentastar's business model, and this whitepaper provides information pertinent to the business aviation customer. The intent is to offer a better understanding of cybersecurity as it relates to business aviation, clarify airliner from business aviation information, and dispel any myths about hacking that can occur on business aircraft.

Within this whitepaper, we will:

- Discuss key differences between internet access systems on airliners versus business aircraft
- Provide an understanding of security safeguards used to ensure network security in-flight and on-ground on business aircraft
- Review tips on how to protect your company and aircraft from unwanted exposure
- Help determine which internet access platform best suits your needs

Pentastar Aviation has a steadfast commitment to safety, and it is the foundation of every aspect of our flight operations. This dedication ensures our clients' aviation experience will always be safe and secure. We vigilantly monitor our clients' aviation programs to safeguard not only their aircraft, its crew, and passengers but also their network assets on board. In fact, our core values of quality, safety, and customer service have allowed us to continuously raise expectations in our industry for more than 50 years.

Pentastar Aviation – Setting the Standard

For more information about our connectivity solutions call us at 248-666-8388 or visit us online at PentastarAviation.com/avionics.

CONNECTIVITY SOLUTIONS from PENTASTAR Aviation

INTERNET ACCESS SYSTEMS

BUSINESS AIRCRAFT ARE DIFFERENT THAN AIRLINERS

In April of 2015, hacker Chris Robert claimed to the Federal Bureau of Investigation (FBI) that he had compromised a jetliner's flight controls at least 15 times by connecting via a seat-base mounted electronics box that was part of the cabin in-flight entertainment system. Robert claimed he was able to assume control of the throttles of the jetliner and alter its flight path. In the age of increased cyber attacks and broadening connectivity, a thorough investigation by the FBI and aviation community was conducted, and Robert's claims were proven to be false.

Late last year a report was also issued from the Department of Homeland Security (DHS) that stated a specialist within the department claimed to have accomplished a "remote, non-cooperative penetration" of a Boeing 757 using standard equipment that can be transported through security. There has been no final report as of yet to validate this claim or document the efficacy of this method. However, it is conceivable that with technological advancements come unintended consequences.

In any case, either of the above claims would not have been possible on the airliner or a legacy or modern business aircraft, as the connectivity systems on board are electrically and physically isolated from all communication, navigation and flight control systems.

Airliners and business/general aviation aircraft also share the similarity that their connectivity systems utilize either "air-to-ground" terrestrial based systems for domestic operations, or a satellite-based system with higher throughput for domestic or international operations. However, that is where the similarities end as modern business jets employ multiple networks, that are physically and electrically separated, for in-flight entertainment and connectivity as well as the central maintenance computer, to make it impossible to "bridge" across networks. Whereas, the latest generation of "fly-by-wire" airliners (Airbus A350, Boeing B787 Dreamliner) employ a common network for critical and utility systems including in-flight entertainment and connectivity. However, these networks are still highly specialized and have numerous safeguards to maintain integrity and defend against hacking attempts and have proven to be impenetrable in the conventional operating environment.

NETWORK SECURITY IN-FLIGHT AND ON-GROUND

SECURITY SAFEGUARDS USED FOR BUSINESS AIRCRAFT

In-Flight Security Safeguards

Whenever the internet is accessed from the aircraft, cybersecurity protection falls on the service provider selected by the aircraft operator. Service providers such as Satcom Direct®, GoGo® Business Aviation, Honeywell's GoDirect™ and Rockwell Collins ARINCDirect℠, to name a few, employ multiple layers of cyber security protection to ensure the integrity and security of the data transmitted across their network. These methods include firewalls, radio network IP concealment, multiple data centers for resiliency, redundancy and failover. They also perform frequent system vulnerability assessments and penetration tests, so the data transmitted to and from the aircraft is protected by all of the pertinent Federal Aviation Administration (FAA) and Radio Technical Commission for Aeronautics (RTCA) requirements, as well as Payment Card Industry Data Security Standard and International Standards Organization (ISO) 27001:2013, and National Institute of Standards and Technology (NIST) industry certifications.

In-flight, protecting the WiFi signal is irrelevant as it is only accessible from inside the cabin of the aircraft, so there is no risk of an external hacker gaining access to the internet, as one could not get close enough to the aircraft to do so.

On-Ground Security Safeguards

When your corporate aircraft is parked at a Fixed-Base Operator (FBO), and electrical power is applied, there is a remote possibility that a sophisticated password crack could occur and access to the WiFi system could result. Although if there are no servers or data storage devices on board the aircraft, and standard security protocols are in place such as firewalls and VPN, data security and network penetration risks are minimal. If your aircraft is equipped with a terrestrial based system such as GoGo® ATG, SmartSky Networks®, and satellite-based Swift64, SwiftBroadBand and Ka/Ku that are physically and electrically isolated from all other systems on the aircraft, the threat of hacking into flight critical systems is also non-existent. However, there is a possible threat if an aircraft is equipped with a satellite-based system (internet access possible while on the ground), that an intruder could run up data service charges by downloading content from the internet, as your aircraft would then be acting as a Wi-Fi hotspot for the intruder.

PROTECTING YOUR COMPANY & AIRCRAFT FROM UNWANTED EXPOSURE

SECURITY SAFEGUARDS YOU SHOULD TAKE

- Use a VPN connection to access internal company systems
- Ensure your company has firewall and cybersecurity protocols in place
- Disable the Wi-Fi system while parked at an FBO. Utilize the “Wi-Fi On/Off” switch that is normally provided in the cockpit
- Disable Wi-Fi router SSID (Service Set Identifier) broadcast and pre-load network connection data onto the devices of travelers
- Ensure that the mobile devices of travelers are adequately secured.
- Frequently change the Wi-Fi password
- Implement a Two-Factor Authentication (2FA) Solution, similar to what you encounter while accessing a Wi-Fi network from a hotel room or other public WiFi network
- Configure your router to only allow data flow while inflight.
- Terminate the internet connection when flying over countries that are known to employ aggressive hacking techniques (Russia, China, etc.)

If your corporate aircraft is used for charter and charter passengers are accessing the internet via the aircraft connectivity systems in-flight, it would not be possible to access your corporate network assuming that standard corporate network security protocols and countermeasures are in place. Just like in your buildings, firewalls and VPN isolation from the public internet are just as imperative on your aircraft. All that is provided to your charter customer is the “coffee shop” type hotspot access experience. As an additional precaution, it would be wise to remove physical property such as company laptops, tablets or devices from the airplane during charter operations.

INTERNET PLATFORMS

WHICH IS BEST FOR YOUR NEEDS

The past several years have seen the development and implementation of several internet access systems. There are the terrestrial based GoGo® and SmartSky Networks® Air-to-Ground (ATG) systems as well as enhancements to legacy Inmarsat High Gain SatCom systems such as Swift 64™ and SwiftBroadband™, and now there are the emerging “Kurz” or Ka/Ku satellite-based high throughput systems. These products can be found on everything from light jets all the way up to large transoceanic capable aircraft. These systems provide

data services to passengers and the flight deck and provide solid and secure access to the internet and corporate virtual private networks.

Things to consider when choosing an internet platform:

- Number of travelers and devices that would be utilizing the data services
- The aircraft's typical mission (domestic North America only, international or a mix of both)
- Bandwidth requirements: are things like textual email messages and small .pdf attachments acceptable? Or is video conferencing, gaming, streaming video content or large file transfers required?
- Service costs
- Service provider's cybersecurity measures and incident rate

CONCLUSION

In conclusion, hacking into or intruding into a business aircraft flight control system is currently a non-existent risk. The largest threat to cybersecurity on business aircraft is targeting the devices of the passengers onboard. However, if the proper precautions are taken to secure the actual devices being used aboard the aircraft, the threat of stealing intellectual property, personal information, or financial information can be mitigated.
At Pentastar Aviation, we believe secure accessibility should have no bounds. That's why our avionics team remains focused on the future of in-flight connectivity. If you have any questions about information contained in this whitepaper or would like more information about Pentastar's avionics solutions, please call us at 248-666-8388 or visit us online at PentastarAviation.com/avionics.

CONNECTIVITY SOLUTIONS from PENTASTAR Aviation