Cybersecurity Challenges in Aviation

by Paul Tyson[1]

In 2015, a group of hackers gained access to one of the world's largest airline's computer networks, causing temporary disruptions that grounded aircraft for several hours. A U.S. government investigation revealed that the hackers had been in the system for over a year before the attacks occurred. Also in 2015, a cyber security consultant told the FBI he had hacked into the in-flight entertainment systems aboard airliners multiple times and was able to issue a command to one of the airplane's engines. The FBI and the airline disputed his claims, but that didn't stop the FBI from executing a search warrant and seizing his laptop computer. Whether or not his claims are true, the fact remains that the thought of a devastating cyber attack on the airline industry has crept into the psyche of the industry and the country's highest law enforcement body. As with every single facet of modern life, the question turns to not "if" but "when" the aviation industry will suffer a catastrophic cyber attack and what can be done to protect this industry and the millions of people who use it every single day?

The aviation industry's impact on the global economy is estimated to be more than $2 trillion, or 3.5% of global gross domestic product. As the aviation industry has become more and more dependent on computer systems, advances in technology and connectivity have boosted aviation safety, efficiency and customer satisfaction. Elements of the industry that rely heavily on connectivity include: flight operations, passenger reservations, cargo handling and shipping, passenger embark/debark procedures, air traffic control systems, and flight control navigation computers, just to name a few. A disruption to the computer systems of any one of

[1] Paul Tyson is an associate attorney at the law offices of Fitzpatrick & Hunt, Pagano, Aubert, LLP in Los Angeles, CA.

these elements could create a devastating domino effect causing economic and social distress around the world. Now more than ever, it is imperative that leaders in aviation, computer security, and the world's regulatory agencies take decisive action to ensure the protection of this vital transportation system.

For the last 10 years, the Federal Aviation Administration (FAA) has been modernizing the Air Traffic Control (ATC) system through its Next Generation Air Transportation System (NextGen), an Internet Protocol (IP) based technology that will replace radio communications with satellite-based communications. While this new technology allows the FAA to efficiently gather and distribute data to effectively conduct ATC functions, ATC systems are now at a greater security risk. Previously, this critical infrastructure was isolated in closed systems and created with proprietary software. With the integration of outside technologies, these systems will use software more familiar to hackers. While the industry has addressed the risk of cyber attacks for some time, the need to find large-scale, workable solutions for these threats to aviation systems is gaining greater and greater urgency.

In 2009, the Department of Transportation (DOT)'s Office of the Inspector General (OIG) sent a report to the FAA that revealed several alarming weaknesses in the FAA's ATC mission-support systems. Web applications had holes that provided "front-door access" that could allow hackers to insert malware onto FAA systems. Intrusion detection systems, that automatically generate security alerts when potential cyber attacks are detected, were only deployed at 11 of the hundreds of operational ATC facilities. The report stated, "[i]n our opinion, unless effective action is taken quickly, it is likely to be a matter of *when*, not *if*, ATC systems encounter attacks that do serious harm to ATC operations."

More recent headlines indicate the problem is only getting worse in the United States and internationally. In 2013, U.S. federal agencies discovered a prolonged operation by state-sponsored hackers to spy on aviation systems at 75 U.S. airports through spear-phishing emails directed at airline personnel. In 2015, a known virus spread via email on the FAA's administrative systems forcing the FAA to alter its competition among contractors to help run the FAA's cybersecurity center. That same year, an entire airport in Warsaw was grounded when a cyber attack disabled the computer systems used to issue flight plans of a Polish airline.

Over the years, the FAA has taken many steps to protect air travel in the United States from cyber-based threats. Nevertheless, a January 2015 report by the Government Accountability Office (GAO) found that "significant security control weaknesses remain, threatening the [FAA]'s ability to ensure the safe and uninterrupted operation of the national airspace system (NAS)." Citing numerous areas of weakness, the report found that as a result of these vulnerabilities, the air traffic system was "at increased and unnecessary risk of unauthorized access, use, or modification that could disrupt air traffic control operations." The GAO issued a follow-up report in April of 2015 telling Congress that the FAA needs a more comprehensive approach to address cybersecurity in the NextGen system.

The threat is not limited to the FAA and the airline industry. On May 9, 2016, the OIG released a report that the Transportation Security Administration (TSA) is failing to comply with the most basic of cybersecurity protocols. The OIG conducted a series of tests of checkpoint operations in real world conditions and the system as a whole: "The failures [found] included failures in the technology, failures in TSA procedures, and human error. We found layers of security simply missing."

These cybersecurity deficiencies in the aviation industry have been noted by Congress. In April 2016, Senator Edward Markey (D-MA) proposed the Cybersecurity Standards for Aircraft to Improve Resilience Act of 2016, or the Cyber AIR Act (S.2764 – 114th Congress) which would require all domestic and foreign air carriers and manufacturers of aircraft or electronic control, communications, maintenance, or ground support systems for aircraft to report cyber attacks to the FAA and for the for FAA to then report to Congress. This bill would further mandate that the FAA incorporate cybersecurity regulations prescribed by the DOT into the requirements for obtaining an air carrier operating certificate or a production certificate. The DOT would require "all entry points to the electronic systems of each aircraft operating in U.S. airspace and maintenance or ground support systems for such aircraft to be equipped with reasonable measures to protect against cyberattacks."

It appears that a proactive approach by the U.S. government, other governments and also international organizations, most likely through the International Civil Aviation Organization (ICAO), is essential to help bring about this much needed change in cybersecurity practices. The worldwide aviation systems are regulated by the aviation authorities in each country, and are both highly structured and highly integrated. This is recognized, for example, in 18 separate ICAO Annexes which attempt to impose uniformity through the implementation of specific Standards and Recommended Practices (SARPs) in every aspect of aviation (e.g. Rules of the Air, Aeronautical Charts, Operation of Aircraft, Airworthiness of Aircraft, etc.). This international regulatory system has been highly effective in fostering the growth of safe air travel. As a result, aviation is statistically one of the safest ways to travel, and this record has improved year after year. Any significant changes in this system, such as those which will be necessary to guard against cyber attacks, must deal with the complexities of the aviation system

both nationally and internationally. And any changes must take account of the fact that the knowledge and culture of the users of the aviation system will require time to safely adapt to whatever changes are implemented. The challenge of the FAA and the aviation industry in the U.S. is to invent new ways of guarding against cyber attacks which merge with a complex existing system.

The rapid growth of cyber attacks shows that fundamental change must occur quickly. The right question is not, "Can they do it?" but rather, "What will it take to make them do it?" Perhaps the Cyber AIR Act will be the catalyst that truly causes change, but these changes have to be internalized at every level of every organization. Whatever it takes, the aviation industry, cyber security industry, and government authorities all need to continue to work together to develop best practices to meet these new challenges to ensure the public's safety.

For more information, please visit the Aircraft Builders Council website at www.aircraftbuilders.com or email info@aircraftbuilders.com