ATCA Aviation Cyber Security White Paper Series Executive Summary

Forming a Strategic Initiative to Combat Modern Cyber Security Threats

Authored by

ATCA's Cyber Security Committee

Problem Statement/Introduction:

Over the past 20 years, cyber security has positioned itself as an independent community in the world of operations. While cyber security is composed of an array of specialists, those specialists must work hand-in-hand with the development and operations team to ensure that irregularities, both small and large, are reported. Reporting is vital in order to execute a well-orchestrated action plan when a cyber threat is suspected. Zero day attacks, in which hackers find a previously unknown path into a software system resulting in a data breach or a technical meltdown, is a recurring news story. Technology on its own cannot mitigate all of these threats. Therefore, it is critical to the safety and efficiency of aviation operations that operational service anomalies be communicated effectively and that a pre-rehearsed process goes into effect immediately to mitigate these violations. No longer should cyber security vulnerabilities be seen as solely a technical responsibility. Operations can play a large part in keeping aviation service available until the impact area is found and mitigated.

The entire aviation industry – Federal Aviation Administration (FAA), airlines, pilots, air navigation service providers (ANSPs), airport authorities, and the private sector – needs an agreed-upon policy to identify system impacts from cyber threats to operations; this is necessary for the ANSPs as well as aviation partners. This effort must be a collaborative one in which ANSPs identify their aviation partners and lead this initiative. Organizations like the Aviation Information Sharing and Analysis Center (A-ISAC) have made great strides in cyber security, but it is just the beginning.

Background:

The March 2, 2015, Government Accountability Office (GAO) report on the FAA's information security status contained 17 recommendations and 168 specific actions. GAO identified problems that are symptomatic of a large and complex enterprise-level IT infrastructure facing a growing number of cyber threats. The air traffic control (ATC) system is a challenge because it regularly interfaces with numerous IT subsystems within FAA, airline operations centers, and airport authorities. Each of these IT subsystems could introduce cyber security vulnerabilities to the others. This is known as inherent risk.

Analysis:

Two types of cyber vulnerabilities exist: known (non-mitigated) and unknown. There is no established fix to protect against unknown vulnerabilities. However, there are ways to harden our systems from vulnerabilities and improve the ability to identify and rapidly respond once a cyber breach occurs. There are three areas to focus actions: 1) the hardening of the systems, 2) the safe connectivity of the community, and 3) the operational response.

In the hardening of the systems, national standards are being developed to better protect against software breaches. As systems are developed, cyber security requirements must be incorporated. In addition, as a system ages, maintaining the best cyber security practices in software development, maintenance, and operation is key.

As aviation moves into a NextGen/SESAR operations environment, the sharing of information (i.e., SWIM and cloud computing) creates joint aviation services, but also increases cyber risk and potential operational impacts. One result of NextGen will be a significant increase in connecting previously disparate ATC equipment types and technologies into FAA networks. While this will lead to an increased effectiveness and efficiency in communications within the ATC system and between aviation stakeholders, it will also introduce new cyber security vulnerabilities through inherent risk. Based on the fact that the National Airspace System (NAS) and stakeholder systems will be exposed to risks never before experienced, special attention should be given to understanding operational service impacts based on these cyber security risks. Safely connecting our aviation community will take coordination and education. The potential negative impact to aviation operations brought on by both known and unknown cyber threats makes it imperative that the aviation industry adopt a highly adaptive operational response capability.

Recommendations:

As the NAS increases connectivity, action should be taken in the three areas where preparing for cyber threats are most effective: 1) the hardening of the systems, 2) the safe connectivity of the community, and 3) the operational response. In addition, a comprehensive approach to simulating successful cyber attacks needs to be agreed upon and rehearsed by all aviation partners – airlines, pilots, and airport authorities. To address these cyber security vulnerabilities in the short and long terms and to prevent a possible major impact from such threats, the Federal government should initiate a comprehensive cyber security program that addresses the following three action areas mentioned above:

1). Hardening of the systems:

- Build in requirements for cyber security from the start with the systems development life cycle (SDLC). Cyber security has become such an issue in recent years that it now needs to be an integral part of the development of a project management plan. It will be easier to combat if it is governed from the onset of a program.

2). Safe connectivity of the community:

- Conduct a case study on the operational impacts based on high-level threats. Aviation industry operations extend beyond the FAA and the NAS and involve the airlines, airports, Department of Defense (DOD), and general aviation. We need a cohesive response to bring the aviation industry up to par on cyber security. An increased awareness of cyber threats throughout the aviation industry is necessary, as well as a robust outline of cyber training, policies, and procedures.
- Create a research and development process that integrates all systems in aviation to eliminate any interoperability challenges that may be induced by cyber security remediations.

3). Operational response:

- Integrate an aviation-comprehensive incident response plan that includes a holistic view of the aviation airspace and impact to the NAS, airlines, and airport services based on the loss of systems, as well as a response plan that integrates with existing FAA, airlines, airports, and DOD response plans.

Summary:

A comprehensive, holistic, and highly adaptive approach to cyber security is critical to the operations of aviation services in the United States and the world. The impact of not addressing these cyber security vulnerabilities in the short and long terms is too significant to ignore. It is a mistake to wait to act until a cyber emergency occurs at the level of the September 11 terrorist attacks or the 2014 Chicago Center fire. Incident response today using separate awareness tools, processes, and policies can impact aviation as a whole on a larger scale than the actual cyber attack. While this paper addresses practices and procedures of the aviation industry, it is merely a first step in defining a holistic approach to combating cyber security vulnerabilities and developing a standardized response to minimize impact during a cyber security event. The entire aviation industry – FAA, airlines, pilots, ANSPs, airport authorities, and private sector – must work together to put the recommendations listed above into practice in order to mitigate cyber security vulnerabilities. Each aviation entity cannot keep aviation secure by itself; security aviation must be a joint venture.