SECURING AIRLINE INFORMATION

Managing Information System-Related Security Risks

By Robert Rencher, Boeing Associate Technical Fellow, and Faye Francy, Boeing Commercial Airplanes

THE ABILITY TO UNDERSTAND AND effectively provide information security services to protect an airline's operational capability, inclusive of aircraft, information, and technology assets, has become an operational requirement for all airlines. Working with the aviation and security industries, Boeing has established a cyber security trajectory to develop and deploy information security solutions for our airlines and the aviation sector.

During the past decade, airlines have made substantial investments in information technology (IT) solutions. These solutions extend throughout the airline's environment and contribute to improved operational efficiency, safety, and customer satisfaction. Securing these investments and protecting the information that these systems manage requires knowledge, leadership, and an effective information security strategy.

The introduction of advanced e-enabled airplanes such as the Boeing 787, 747-8, and other OEM digitally enabled aircraft provide an increased level of operational efficiency to the airlines. This also means an increased interaction with many information systems that are both on board the aircraft and on the ground that operate outside the traditionally defined airline network security perimeter.

This article provides an overview of airline information security, outlines the requirements for an information security framework, discusses how digital airplanes influence airline information security, and describes Boeing's proposed information security strategy.

Airline Information Security

Well-defined information security strategy safeguards airline customer information, protects the airline's digital assets, and enables the accurate exchange of information within the industry. A holistic approach to information technology solutions follows a mature security discipline to protect the airlines' information and those

Photographer: Maksim Kabakou/Photos.com

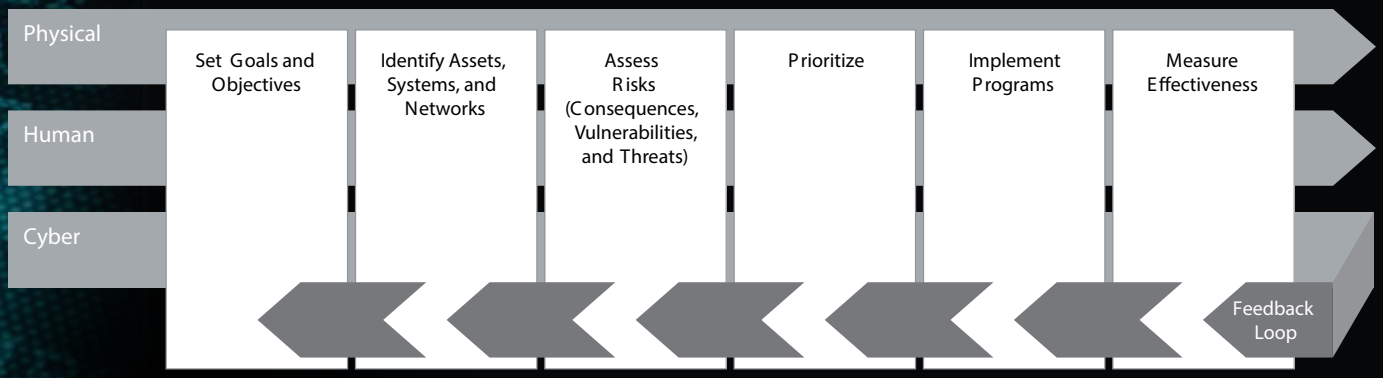

Figure 1: Effective information security strategy

business partners with whom they interact.

Pervasive and instantaneous network connectivity, once limited to IT environments, is now part of the global aviation culture. Airline information systems, advanced technology airplanes, and other aviation industry solutions collectively utilize this connectivity to communicate information, create awareness, and report on the status of the operational environment. The integrity of this aviation digital framework requires that all participants adopt and utilize effective information security strategies that are focused on continuous improvement against cyber threats (see Figure 1).

Collaboration within the aviation industry defines, promotes, and ensures that information security best practices are protecting the industry's information assets.

Continuous improvement of information security strategies is essential for the most effective protection of critical data.

A Robust Information Security Strategy

The commercial aviation industry will benefit from a closed, protected forum in which industry and government can exchange information about emerging cyber threats and best practices to the aviation industry.

This forum would engage key government and industry participants in the development of appropriate, coordinated strategies, policies, standards, and processes for aviation. The establishment of such a forum will enable the industry to understand the capabilities of existing and planned cyber security controls, and assure that it is prepared for the continuing emergence and escalation of cyber security threats to information.

To enable this forum an Aviation Information Sharing and Analysis Centers (A-ISAC) is being established by aviation leaders as sanctioned by the Aviation Sector Coordinating Council (A-SCC). Its mission is to advance physical and information security sharing across the aviation sector and to coordinate and collaborate around the world with like-minded companies, suppliers, airports, airlines and other related organizations to establish and maintain a framework for interaction between and among aviation stakeholders and with governmental entities.

Developing an Airline Information Security Framework

The need for airlines to adopt a solid information security framework is clear. Cyber attacks are increasing in number and sophistication and software vulnerabilities expose intellectual property to unauthorized users. Malware, botnets, and insider threats expose the aviation infrastructure to potential nefarious actions by malcontents.

Effective information security risk management requires a framework and methodology that can adjust to this dynamic security threat environment. An airline information security framework ensures that:

- Managing information system-related security risks is consistent with the organization's mission, business objectives, and overall risk strategy established by the airline's senior leadership.
- Information security requirements – including necessary security controls – are integrated into the airline's enterprise architecture and system development lifecycle processes.

The ideal airline information security framework addresses airplanes in flight, ground operations, and threat management; and consists of three major functions: prevention, detection, and response (see Figure 2).

Prevention addresses the ability to prevent disruption to the current operational state by allowing authorized access to the system services and stopping unauthorized access. Creating awareness and providing education are key elements of prevention.

Detection consists of the ability to detect a security threat and assess information systems' vulnerability to threats. Security threats consist of all methods, both intentional and unintentional, that result in unauthorized use of information systems. Detecting a threat requires a methodology and set of tools to define and evaluate the authorized access and use of the information systems and the detection of information system abnormalities.

Response comprises of timely and effective communication to a defined set of stakeholders and the initiation of countermeasures to thwart the active threat to reconcile disruptions and recover the system.

An effective airline information security framework continually prevents, detects, and responds to security threats.

The information security framework is supported by three qualifying concepts: defense in depth, active management, and configuration control.

Image courtesy of: Boeing

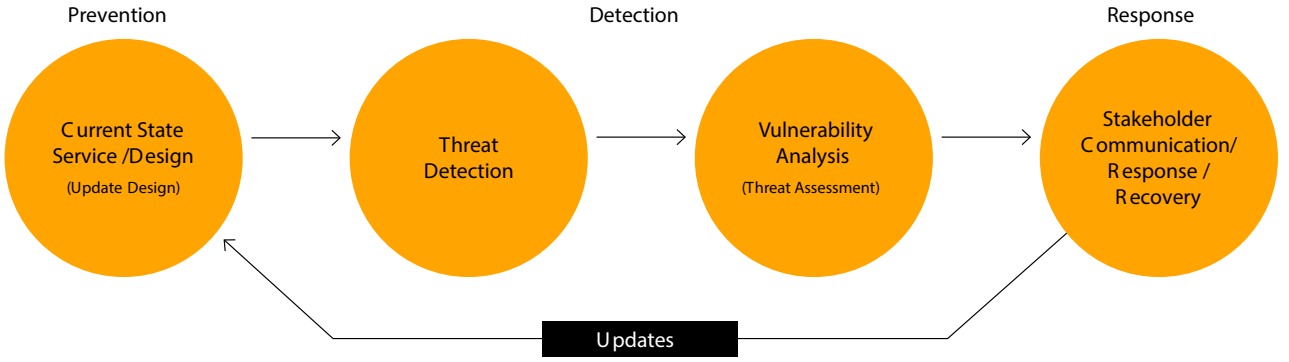

Figure 2: Prevention/detection/response model

Defense in depth addresses the need to establish a multi-layered approach to ensure that prevention, detection, and response cannot be compromised with a single threat approach or disruption event.

Active management is the persistent awareness of the network and its configuration. Both scheduled and un-scheduled events occurring on the network that would change the configuration of the network are tracked.

Configuration control is the adherence to a well-documented process that manages all changes to the information system. This change control process falls under the broader discipline of business continuity.

How Digital Airplanes Influence Airline Information Security

As the connectivity of aviation services and inclusion of information technology services continues to increase, so does the potential for security vulnerabilities. Information security threats to commercial aviation present some unique challenges.

For example, several security challenges can threaten an entire fleet of airplane types. These threats can manifest themselves as internal security deficiencies or attacks from external sources such as the supply chain and network connections within the industry.

The existing in-service fleet of airplanes contains computerized systems, software parts, software control of devices, and off-board communication capabilities that all require an effective security solution.

In conjunction with the aviation industry and information security industry, Boeing is developing a holistic cyber security aviation framework that addresses airplane and ground systems and addresses the threat management component (see Figure 3). The aviation security framework includes the identification and definition of emerging threats, guidelines for incident response, and conducting forensic analysis of the threat. The dotted, dashed and solid lines define the actions taken to address a cyber threat. The dotted line indicates that a new requirement has been identified. This initiates a series of events and activities to validate and evaluate the threat profile resulting in an update to the security threat repository. This security threat repository is a collaborative non-industry specific resource. Requirements may also emerge from an incident response. The dashed line indicates a threat requires an incident response. This is an active threat and is addressed in real-time. The solid line indicates a non-aviation related security threat. These threats are monitored for future analysis in the event there is a use of this threat within the aviation industry.

Boeing's holistic cyber security aviation framework is designed to address both airborne and ground-based cyber threats. The aviation industry benefits from the availability of a cyber security information resource that provides a protected venue for exchanging sensitive security information.

The proposed aviation industry cyber security aviation framework includes an information sharing and analysis center (ISAC) that provides the industry with a unique and specialized forum for managing risks to the aviation infrastructure. Members can participate in conjunction with national and security efforts to strengthen the infrastructure by sharing information and analyzing physical and cyber threats. As a result, airline members would help other airlines and industry-related companies improve their incident response through trusted collaboration, analysis, and coordination. This will facilitate decision-making by policy makers on security, incident response, and information sharing issues.

Boeing Information Security Solutions

To support industry collaboration, Boeing is working with industry to help establish a unified cyber strategy and deliver cyber security solutions to airlines worldwide. This includes establishing a center of excellence for cyber-secure-network-based solutions—including methods, standards, technology, training, and performance.

To develop these solutions, a secure center for cyber security research environment has been established that is focused on the A-ISAC, securing airborne networks and the global aviation infrastructure. This will provide as access to aviation experts that can support:

- Conducting cyber threat and vulnerability assessments of airborne systems.
- Designing cyber protection for commercial airplanes.
- Supporting the development of industry standards for aviation security.
- Monitoring and detecting cyber events.

Image courtesy of: Boeing

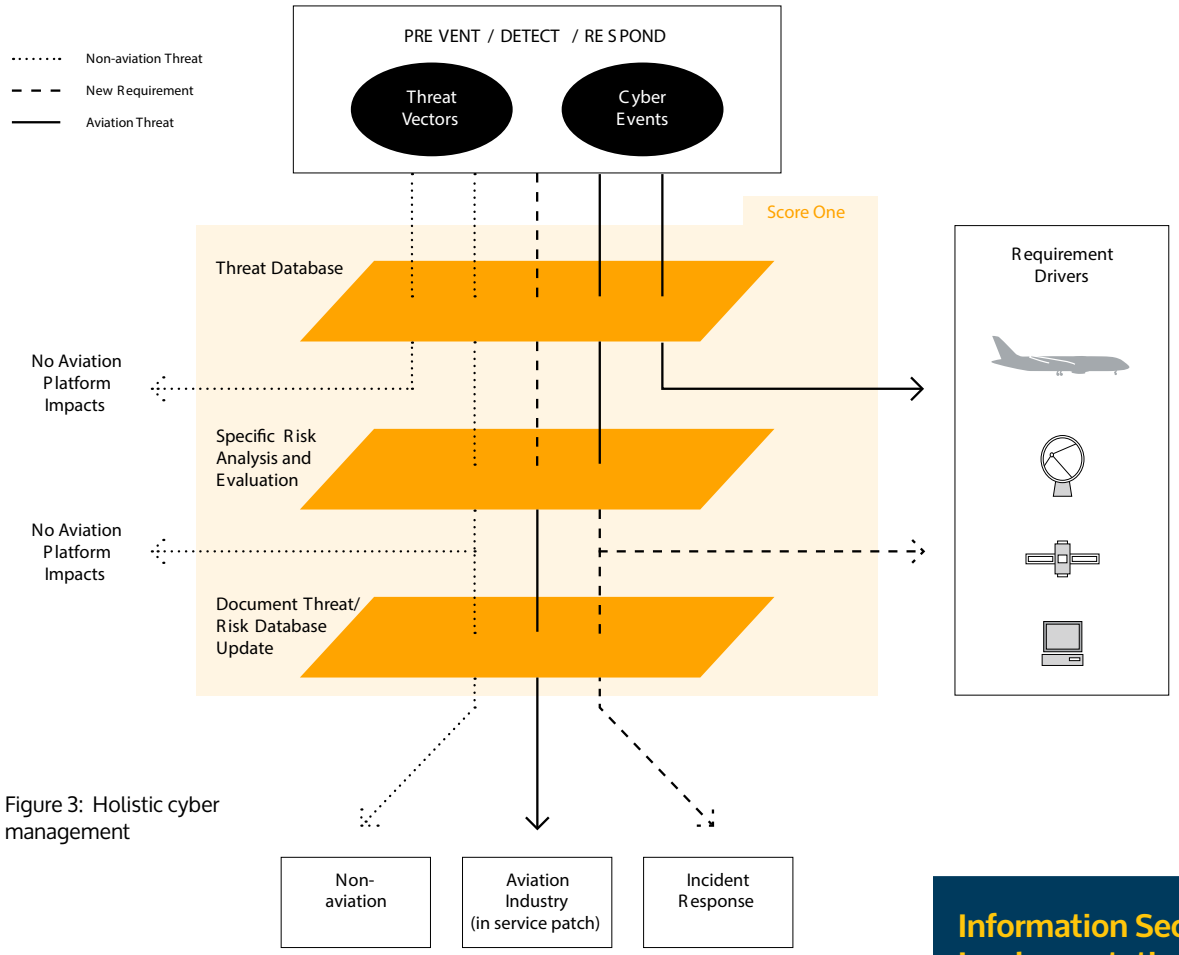

Figure 3: Holistic cyber management

- Offering cyber response and protection services to airline customers.
- Persistent network mission assurance combined with knowledge management for safe and efficient operations, creating increased shared situational awareness.

Awareness Summary

As airlines continue to make substantial investments in IT systems, securing these investments and protecting the information that these systems manage is critical. The increasing number of e-enabled airplanes makes an effective information security strategy even more important.

About the Authors

Robert Rencher *is a Senior Systems Engineer responsible for defining and establishing the information technology strategy for Boeing Commercial Aviation Services. This information technology strategy defines both the business opportunity and technology requirements in support of the airlines operating Boeing airplanes. As such, Rencher's emphasis includes addressing the emergent cybersecurity challenges to the aviation industry. Contributions to the industry include International Air Transport Association, National Institute of Standards and Technology, Network Centric Operations Industry Consortium, and The American Institute of Aeronautics and Astronautics.*

Faye Francy *is the leader of the Boeing Commercial Airplanes (BCA) Cyber ONE team. This team is an enterprise-wide Community of Excellence (CoE) group that is working together across the Boeing Company focused on leveraging the best of Boeing in the cyber domain. Francy is developing and coordinating a public-private partnership with the aviation industry and the U.S. Government to support establishing an Aviation Information Sharing Analysis Center (A-ISAC).*

For more information, please contact Robert Rencher (robert.j.rencher@boeing.com) or Faye Francy (faye.i.francy@boeing.com).

Information Security Implementation Strategy

The implementation strategy for airline information security follows a systematic escalation of system and geographic transition. This requires the prioritization of airline systems. Systems that are deemed as non-critical are evaluated first for demonstrating the process of transitioning to the proposed information security solution. This approach limits the risk exposure to the airline's critical operation systems.The transition of systems from one region to another must take into consideration the requirement of inter-regional operations. The first geographic priority is to evaluate the autonomy of one area airline region. As two regions have validated the implementation of non-critical system implementation, these two regions must then validate the interoperability of non-critical systems. This again demonstrates the capability without putting to risk critical systems.