Boeing is working with industry to establish a unified cyber strategy and deliver cyber security solutions to airlines worldwide.

Securing Airline Information on the Ground and in the Air

The ability to understand and effectively provide information security services to protect an airline's information and technology assets has become an operational requirement for all airlines. Working with industry and together across the enterprise, Boeing has launched a cyber security effort to develop information security solutions and provide them to airline customers.

By Robert Rencher, Senior Systems Engineer, Associate Technical Fellow;
Stephen Whitlock, Chief Information Security Strategist, Technical Fellow; and
Faye Francy, BCA Enterprise Cyber Security One Team Leader

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 will provide an increased level of operational efficiency to the airlines. However, this means increased interaction with many information systems that are outside the traditionally defined airline 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 information security strategy.

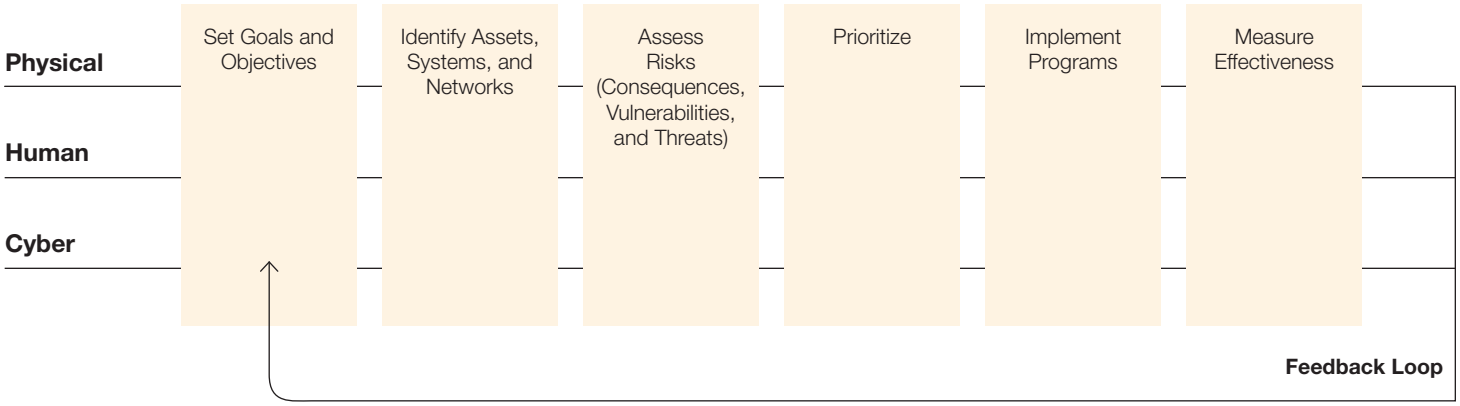
AIRLINE INFORMATION SECURITY

Having and following a well-defined information security strategy safeguards airline customer information, protects the airline's digital assets, and enables the accuracy of information exchanged within the aviation framework. Boeing's holistic approach to IT solutions follows a mature security discipline to protect both Boeing's and the airlines' information.

Pervasive and instantaneous network connectivity, once limited to IT environments, is now part of the global aviation culture. Airline information systems, Boeing's advanced technology airplanes, and other aviation industry partners 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

Figure 1: Effective information security strategy

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



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 noncritical 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 noncritical system implementation, these two regions must then validate the interoperability of noncritical systems. This again demonstrates the capability without putting critical systems at risk.

requires that all participants adopt and utilize effective information security strategies that are focused on continuous improvement to guard against cyber threats (see fig. 1).

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

BOEING INFORMATION SECURITY STRATEGY

Boeing believes the commercial aviation industry could benefit from a closed, protected forum in which industry and government can exchange information about emerging information security cyber threats to the air transport and aviation industries.

This type of forum would engage key government and industry participants in the development of the 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 the aviation industry.

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. Software vulnerabilities expose intellectual property to unauthorized users. And insider threats to IT infrastructure and proprietary information are increasing.

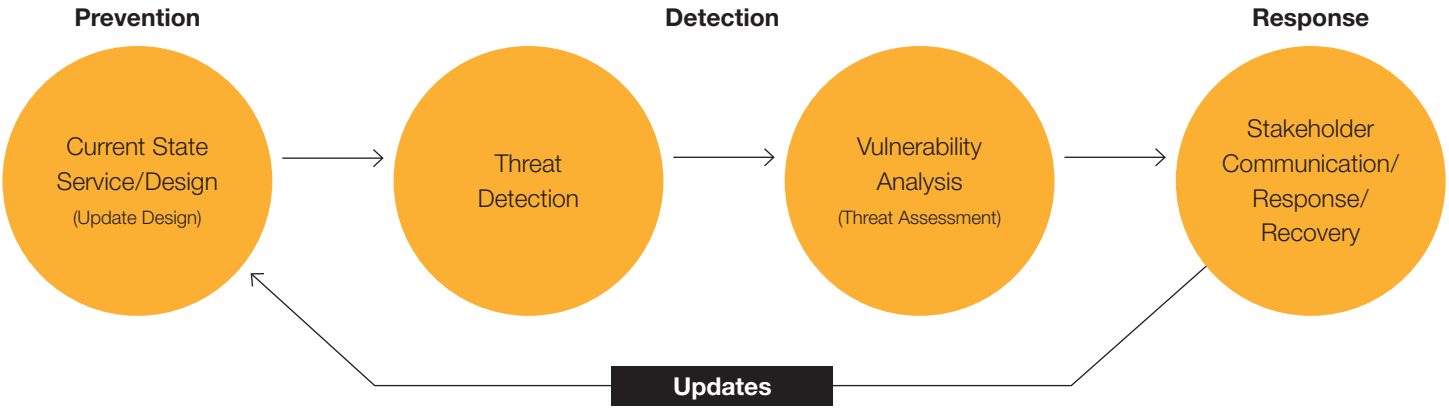
Effective information security risk management requires a framework and methodology that can adjust to this dynamic security threat environment. An airline information security framework should ensure that:

- 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. It consists of three major functions: prevention, detection, and response (see fig. 2).

Figure 2: Prevention/detection/response model

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



- Prevention addresses the ability to prevent disruption to the current operational state by allowing authorized access to the system services and preventing unauthorized access.
- 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 use of the information systems and detect information system abnormalities.
- Response comprises timely and effective communication to a defined set of stakeholders and the initiation of countermeasures to thwart the active threat and to reconcile disruptions and recover the system.

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

- Defense in depth addresses the need to establish a multilayered 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 unscheduled 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 continues to increase, so does the potential for security vulnerabilities. Information security threats to commercial aviation present some unique challenges.

For example, 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.

Boeing, in conjunction with the aviation industry and the information security industry, is developing a holistic cyber security aviation framework that addresses airplane and ground systems and has a threat management component (see fig. 3).

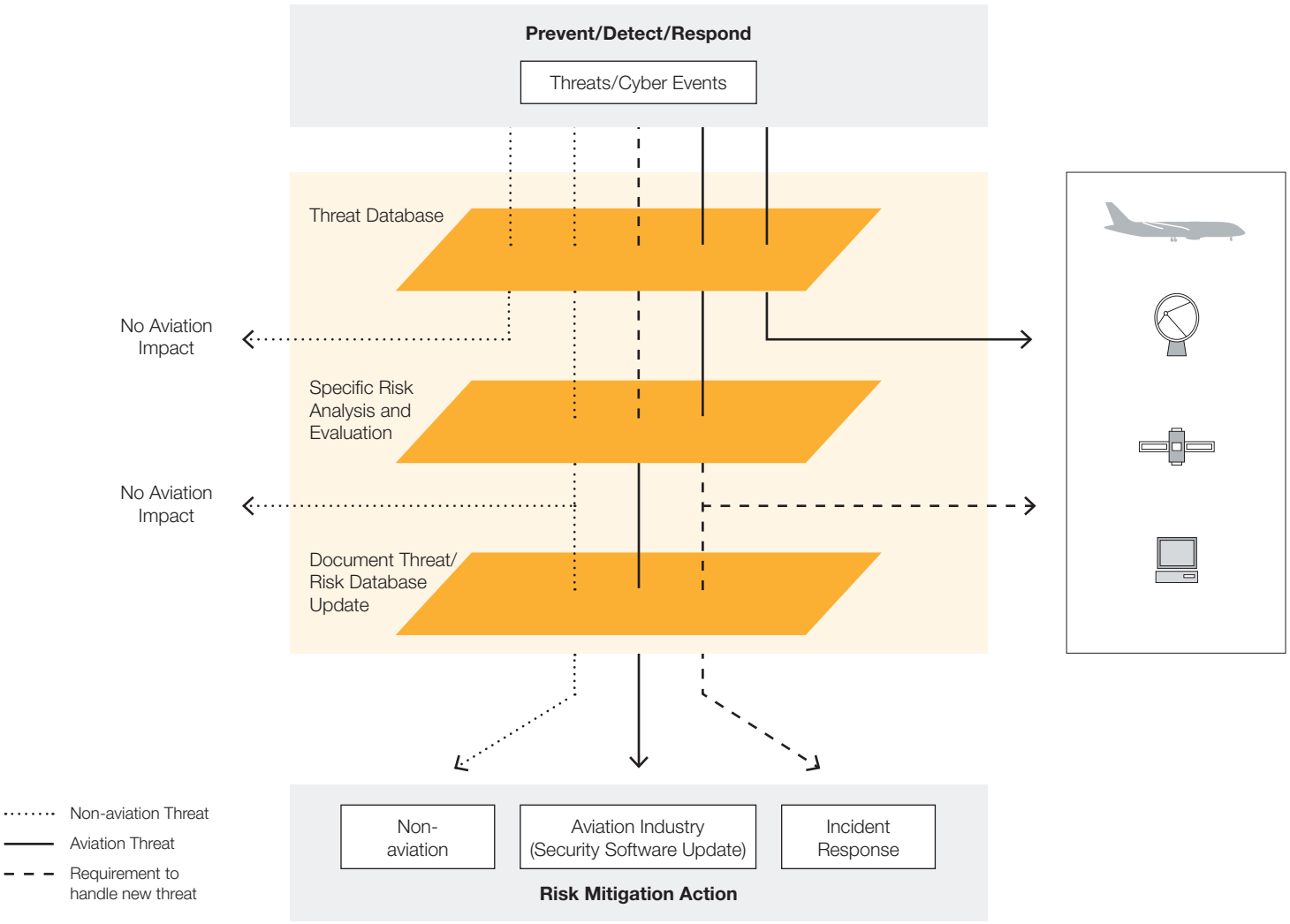
The aviation security framework includes defining emerging threats, guiding incident response, and conducting forensic analysis. These response and analysis services are available through CAS Professional Services.

Boeing's cyber security aviation framework includes the development of an aviation information sharing and analysis center (ISAC) that provides the aviation 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 aviation infrastructure by sharing information and analyzing physical and cyber threats. As a result, airline members will help their companies improve their incident response through trusted collaboration, analysis, and coordination. This will help facilitate decision making by policy makers on security, incident response, and information-sharing issues.

Boeing is committed to establishing an aviation ISAC (A-ISAC). Its mission would be to advance the physical and information security of the aviation industry and to coordinate and collaborate around the world with like-minded organizations to establish and maintain a framework for interaction between and among aviation stakeholders and with governmental entities.

Figure 3: Holistic cyber management

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.



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 — for Boeing commercial airplane systems.

To develop those solutions, Boeing is establishing a Cyber Technical Center that focuses on establishing the ISAC. The Boeing Cyber Technical Center will provide services such as:

- Conducting cyber threat and vulnerability assessments of airborne systems.
- Designing cyber protection for Boeing commercial airplanes.
- Supporting the development of industry standards for aviation security.
- Monitoring and detecting cyber events.
- Offering cyber response and protection services to Boeing airline customers.

Boeing's cyber security team will provide the means of persistent network mission assurance combined with knowledge management for safe and efficient operations, creating increased value for Boeing customers.

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.

Boeing is actively developing a cyber security aviation framework and Cyber Technical Center to support the cyber security needs of our airline customers.

For more information, please contact Robert Rencher at robert.j.rencher@boeing.com.