Deloitte.

Please Fasten Your Seat Belts:
Managing digital risk to support aviation innovation

The typical discussion of cyber attacks usually revolves around stolen credit card data, breaches of personal information, and identity theft. However, an increasing number of companies have been hit with cyber attacks that extend well beyond the typical breach of employee or customer data. This new breed of cyber attack can target intellectual property, strategic plans, and information about high profile people – or can be intended to cause operational chaos, destruction of corporate assets, or significantly threaten public infrastructure and safety. These are not traditional 'hackers' or cyber criminals. They can be nation-state actors or groups with a competitive, political or ideological agenda. While perhaps not considered acts of full-blown cyber terrorism, the latest cyber attacks are arguably entering the realm of cyber terrorism and cyber warfare in their scope and potential impact.

Cyber risk is clearly no longer just about securing corporate data and maintaining data confidentiality, integrity, and availability. Cyber risk is a business risk, even an existential one to some organizations, and can no longer be relegated solely to the domain of information technology (IT) to address. Cyber incidents can disrupt day-to-day operations, impose irreparable reputation damage, and, for the aviation industry, even threaten lives. Corporate boards around the country are asking: Is my company going to be targeted? For aviation companies – in the business of transporting millions of people safely with 100,000 daily flights at 37,000 feet – the stakes are especially high.

The innovation link

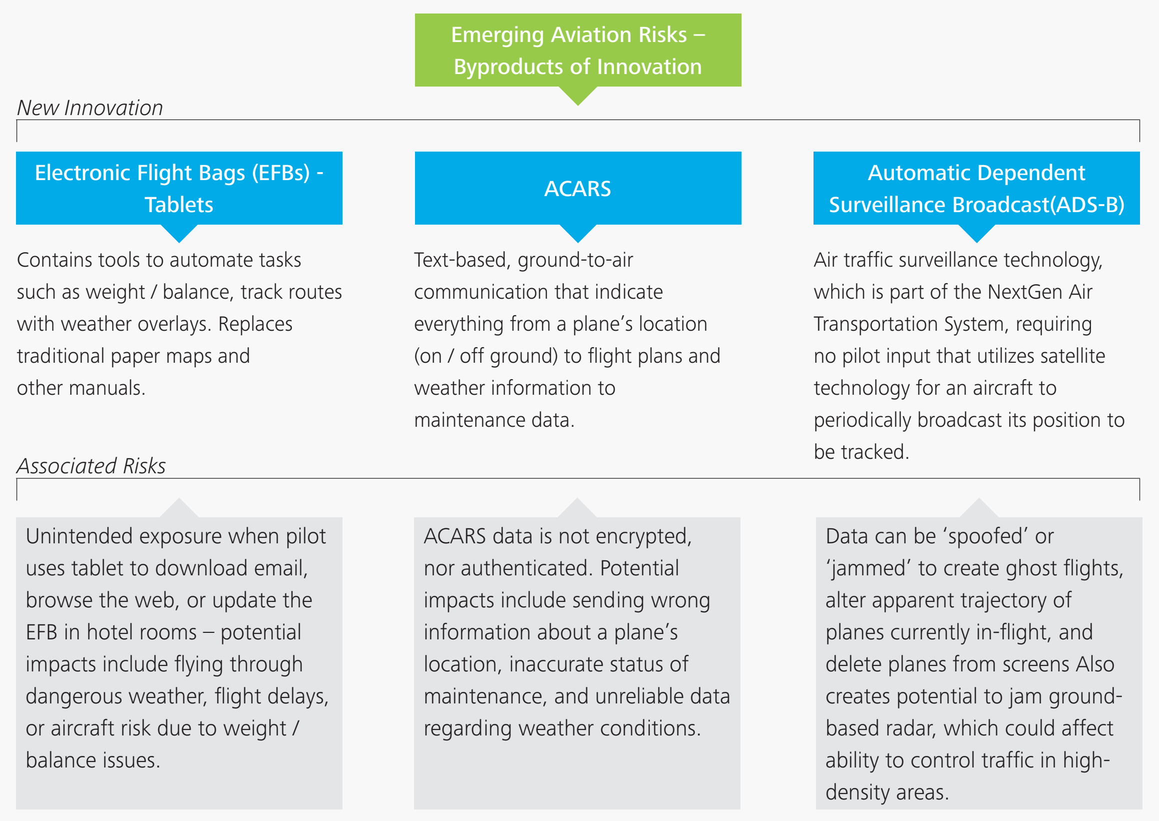
The importance of the aviation industry to the nation's economy cannot be understated. The growth rate of civil aviation has outpaced the overall growth of the US national economy. Based on data collected during the last census in 2012, aviation accounted for 5.4% of the country's gross domestic product (GDP), contributed $1.5 trillion in total economic activity, and supported 11.8 million jobs.[1] As with many sectors, technology innovation is fueling this business performance, as companies have looked to increase operational efficiencies, adapt to consumer demand for online and highly personalized experiences, and introduce new revenue streams through internet-based, value-added services. But with technology innovations, new and increasingly worrisome cyber risks are introduced.

[1] The Economic Impact of Civil Aviation on the U.S. Economy – June 2014 (U.S. Department of Transportation – Federal Aviation Administration)

Rise of the digital aircraft

The new generation of aircraft is IP-enabled, also referred to as “e-enabled” or digital aircraft. These are the “smart devices” of the aviation industry, which are radically changing the way airlines operate from the flight deck, to the cabin, and on the ground. These new innovations, some driven by aircraft technology, others by the handheld digital age, allow the industry to address longstanding operational inefficiencies to optimize fuel consumption, advance maintenance efficiency, improve scheduling, and increase access to real-time quality data through capabilities such as GateLink (PKI), Electronic Flight Bags (EFB), Secure Aircraft Communications Addressing and Reporting System (“ACARS”)[2], and next generation air traffic control. The benefits of these technology innovations are undeniable and pervasive, but they are not without risks, as depicted below.

Figure 1 Potential risks of new aviation technological innovations



Emerging Aviation Risks – Byproducts of Innovation

	Electronic Flight Bags (EFBs) - Tablets	ACARS	Automatic Dependent Surveillance Broadcast(ADS-B)
New Innovation	Contains tools to automate tasks such as weight / balance, track routes with weather overlays. Replaces traditional paper maps and other manuals.	Text-based, ground-to-air communication that indicate everything from a plane’s location (on / off ground) to flight plans and weather information to maintenance data.	Air traffic surveillance technology, which is part of the NextGen Air Transportation System, requiring no pilot input that utilizes satellite technology for an aircraft to periodically broadcast its position to be tracked.
Associated Risks	Unintended exposure when pilot uses tablet to download email, browse the web, or update the EFB in hotel rooms – potential impacts include flying through dangerous weather, flight delays, or aircraft risk due to weight / balance issues.	ACARS data is not encrypted, nor authenticated. Potential impacts include sending wrong information about a plane’s location, inaccurate status of maintenance, and unreliable data regarding weather conditions.	Data can be ‘spoofed’ or ‘jammed’ to create ghost flights, alter apparent trajectory of planes currently in-flight, and delete planes from screens Also creates potential to jam ground-based radar, which could affect ability to control traffic in high-density areas.

Boeing’s new 787 Dreamliner, newer generations of its 777 long-range wide-body aircraft, and Airbus’ A380 and new A350XWB, are already digitally enabled. Older generations of commercial aircraft such as legacy Boeing 737 and 777 models, as well as the Airbus A320 family, are being retrofitted with these capabilities. These modern commercial aircraft have essentially become flying industrial control systems – remote, computer-controlled devices that transport millions of people daily for both business and leisure travel. Each aircraft operates as complex, and potentially hackable, infrastructure of interconnected information technology systems, relying on fly-by-wire and legacy ground-to-air systems to provide flight instructions, identify aircraft weight and balance issues, locate other planes, and avoid dangerous weather.

[2] Wikipedia.org, Aircraft Communications Addressing and Reporting System, http://en.wikipedia.org/wiki/Aircraft_Communications_Addressing_and_Reporting_System, (Mar 21, 2015).

Traditional threats remain

The industry is still exposed to more familiar cyber risks. E-commerce is the aviation industry's primary sales platform. With the development of sophisticated online sales channels and rewards programs, airlines have become increasingly reliant on Internet-based data exchange to transact and promote their businesses. Airlines such as Southwest and JetBlue sell nearly 100% of their tickets directly to customers, avoiding third party Online Travel Agencies (OTAs) altogether. Loyalty program IDs and payment card information (PCI) are used to link consumers to their reservations, and may be stored and accessed by a range of other services, including executive club memberships, seat upgrades, and baggage check-in services, across a range of devices like in-airport kiosks, consumer handheld devices and gate agent kiosks. A gate agent or automated kiosk can access a customer's entire profile and itinerary using one piece of personal identification information (PII). A cyber breach involving a single identifier, or a rudimentary social engineering attack, opens the possibility that a malicious actor could find out exactly where individuals are traveling to and from, when they will arrive, and even which gate they will be arriving at. In the hands of a spy, a stalker, or a kidnapper, this information could threaten passenger safety, and expose airlines to new sources of potential liability. Airlines are already dealing with impersonation of frequent flyer accounts and the theft of loyalty program points. On top of that, they struggle to continually balance the ease of experience with the application of typically non-consumer friendly security controls.

Aviation as critical infrastructure

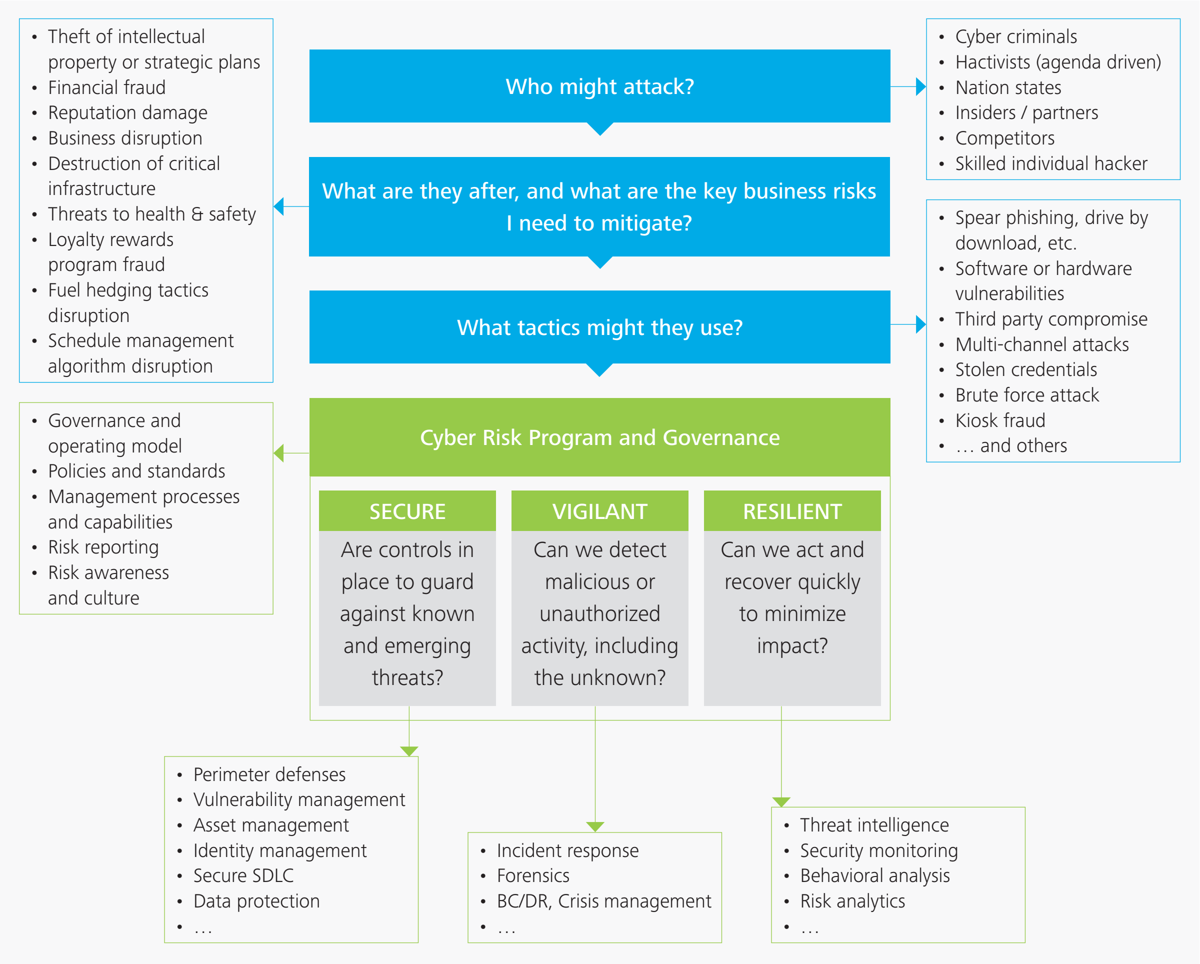
In February 2013, President Obama issued Executive Order 13636 "Improving Critical Infrastructure Cybersecurity," which identified aviation as a critical infrastructure sector. The order directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework, based on existing standards, guidelines, and practices, to reduce cyber risk to critical infrastructure. A year later, NIST released its first version of the "Framework for Improving Critical Infrastructure Cybersecurity," which provides a prioritized, flexible, cost-effective, and repeatable approach to managing cybersecurity-related risk. While the Government's prioritization of aviation has helped shine a spotlight on the sector and has begun to stimulate important discussion, many questions remain about what a comprehensive and effective program looks like in both design and practice for commercial airlines.

Getting ahead of the new threats

An effective cyber risk program should consider the unique set of cyber threats to which the organization is exposed, or cyber threat landscape, to set realistic goals that can and should be achieved with a broad, well-maintained cyber risk framework. No environment is completely secure, nor is it cost effective to try to make it so. An organization should not only take reasonable steps to protect its data, applications, and infrastructure, but should also minimize the damage of successful attacks, and return to normal operation as soon as possible. To effectively manage cyber risk, an organization must put in place a *Secure.Vigilant.Resilient.*™ program.

- Being secure means protecting critical assets against known and emerging threats
- Being vigilant means maintaining threat awareness and detecting adversarial activity
- Being resilient means recovering quickly when incidents occur

Figure 2 Understand who might want to attack, why, and how



Who might attack?

- Cyber criminals
- Hactivists (agenda driven)
- Nation states
- Insiders / partners
- Competitors
- Skilled individual hacker

What are they after, and what are the key business risks I need to mitigate?

- Theft of intellectual property or strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety
- Loyalty rewards program fraud
- Fuel hedging tactics disruption
- Schedule management algorithm disruption

What tactics might they use?

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Stolen credentials
- Brute force attack
- Kiosk fraud
- … and others

Cyber Risk Program and Governance

- Governance and operating model
- Policies and standards
- Management processes and capabilities
- Risk reporting
- Risk awareness and culture

SECURE

Are controls in place to guard against known and emerging threats?

- Perimeter defenses
- Vulnerability management
- Asset management
- Identity management
- Secure SDLC
- Data protection
- …

VIGILANT

Can we detect malicious or unauthorized activity, including the unknown?

- Threat intelligence
- Security monitoring
- Behavioral analysis
- Risk analytics
- …

RESILIENT

Can we act and recover quickly to minimize impact?

- Incident response
- Forensics
- BC/DR, Crisis management
- …

Secure: Protection against known and emerging threats across the ecosystem

An effective security program should continually innovate to protect critical assets against known and emerging threats across the enterprise. While it may not be possible to eliminate the use of credit card numbers to identify reservations, airlines can utilize tokenization technologies to avoid proliferating data such as credit card numbers, social security numbers, known traveler IDs, and passport numbers throughout the environment. Consumers demand a mobile experience for boarding passes, to change seats and request upgrades, to book reservations and for myriad other, authenticated interactions. Public Key Infrastructure (PKI) technologies may be used to encrypt mobile traffic and automate authentication for consumers, increasing security of mobile transactions transparently to the consumer experience. Business units are rapidly partnering with third parties for various services, requiring that vendors have access to specific IT assets. Federation technologies enable business partners to securely access resources without the business exposing sensitive internal directories or taking on the burden of managing third party identities and credentials.

Vigilant: Pre-emptive visibility and situational awareness

Breaches will occur; preventing successful attacks is no longer as simple as patching systems and updating intrusion detection signatures. The ability to rapidly identify attacks is essential in containing the damage they can inflict. A security operations center (SOC) that is integrated into both sensitive applications for detection and security technologies, such as identity management and network access control, for control is the core of an organization's ability to be vigilant for and respond to cyber threats. To be truly effective, the SOC needs to be supported by a Cyber Incident Response Team (CIRT), which monitors, assesses, and escalates incidents. The SOC also continuously refines use-cases to reduce false positives and to optimize log storage for capacity and forensic analysis. In many cases, the SOC can identify emerging threats based on advanced threat intelligence from multiple industry, law enforcement, and other governmental information sharing and analysis centers (ISACs). Non-profit organizations such as the Aviation Information Sharing and Analysis Center (A-ISAC) are designed specifically for this purpose by providing industry-focused functions to protect aviation businesses, operations and services globally.

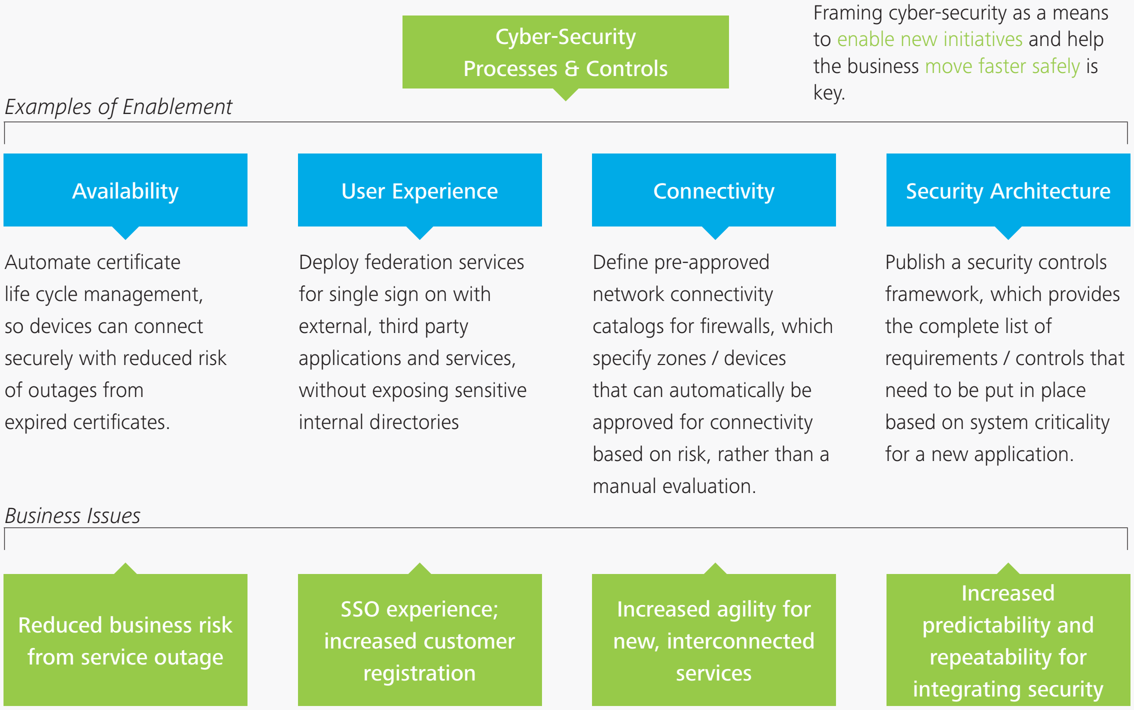
Resilient: Capability to recover when incidents occur.

Given the nature of the business and inherent risks to passenger safety, the majority of airlines are well-versed in incident response and crisis management. However, the threat that cyber attacks pose are far different and in some cases, far more complex, than the traditional safety issues that the aviation industry has experienced, and beyond what many are prepared for. Airlines can prepare for these new threats by rehearsing response to attack scenarios through cyber war gaming. Cyber war gaming involves “tabletop exercises” that emulate actual and possible cyber threats to an organization to understand how effectively the organization responds. These exercises involve all levels of the organization, including business leaders, technical teams, legal counsel, and external parties such as law enforcement and independent third parties, to assess how effectively they interact to manage what can often be substantial ongoing business recovery efforts. Typically, the greatest shortcomings exposed during these exercises are lack of familiarity and preparedness by executive teams, and lack of coordinated response across the many functions within the organization.

Make the business case to position cyber risk efforts as enablers

An effective— and funded—secure, vigilant and resilient cyber program must have visibility at the C-Suite level. Cyber risk is a business risk, and must be considered when an airline evaluates its overall enterprise risk to make business decisions. Savvy CISOs and CSOs are able to position their cyber risk program as an enabler, rather than purely as a necessary evil to maintain compliance. Each investment should have an associated business case, with clear identification and quantification of both enterprise risk reduction and business benefits, which may include for example, improvements in customer experience, operational efficiency through automation of provisioning and governance processes, avoidance of costly, mandated security controls for sensitive data through tokenization technologies, and providing greater agility to support partnering with external vendors.

Figure 3 Potential business benefits from cyber risk investment



Cyber-Security Processes & Controls

Framing cyber-security as a means to enable new initiatives and help the business move faster safely is key.

Examples of Enablement

Availability

Automate certificate life cycle management, so devices can connect securely with reduced risk of outages from expired certificates.

User Experience

Deploy federation services for single sign on with external, third party applications and services, without exposing sensitive internal directories

Connectivity

Define pre-approved network connectivity catalogs for firewalls, which specify zones / devices that can automatically be approved for connectivity based on risk, rather than a manual evaluation.

Security Architecture

Publish a security controls framework, which provides the complete list of requirements / controls that need to be put in place based on system criticality for a new application.

Business Issues

Reduced business risk from service outage

SSO experience; increased customer registration

Increased agility for new, interconnected services

Increased predictability and repeatability for integrating security

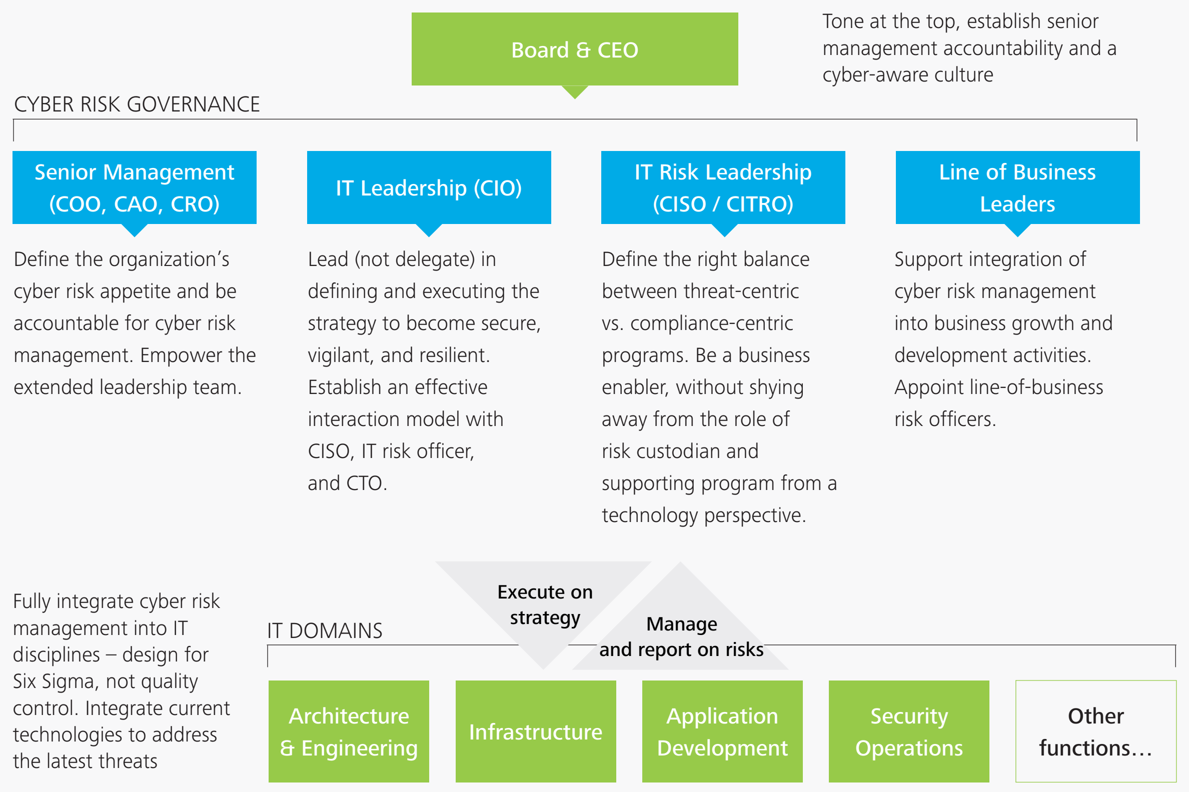
The financial benefits can be direct; for example, insurers provide a material break (discount) on cyber insurance for well-developed security programs – cost savings that flow directly out of general and administrative expenses and go straight to the bottom line.

In a highly concentrated and heavily competitive industry like aviation, where everybody is seeking new technology to improve efficiency, margins, and customer experience, the goal of a robust cyber risk program is to enable an organization to move faster, safely. Such a program not only facilitates, but can accelerate, business initiatives by ensuring that the appropriate processes and procedures are in place for mainstream enterprise adoption and implementation of new technology.

Take it to the top – executive sponsorship and corporate governance is key

Cyber security leaders should have a seat in every meeting of the board to discuss cyber risk in the context of enterprise risk. The board should understand cyber security, and meetings should include regular and consistent reviews of cyber risks along with the overall state of security. Another leading practice is the formation of a 'risk management committee' that comprises multi-functional department heads, including internal audit, flight operations, insurance, legal, and, information security, that meet regularly to discuss cyber risk.

Figure 4 Cyber risk governance structure and executive sponsorship



Board & CEO

Tone at the top, establish senior management accountability and a cyber-aware culture

CYBER RISK GOVERNANCE

Senior Management (COO, CAO, CRO)

Define the organization's cyber risk appetite and be accountable for cyber risk management. Empower the extended leadership team.

IT Leadership (CIO)

Lead (not delegate) in defining and executing the strategy to become secure, vigilant, and resilient. Establish an effective interaction model with CISO, IT risk officer, and CTO.

IT Risk Leadership (CISO / CITRO)

Define the right balance between threat-centric vs. compliance-centric programs. Be a business enabler, without shying away from the role of risk custodian and supporting program from a technology perspective.

Line of Business Leaders

Support integration of cyber risk management into business growth and development activities. Appoint line-of-business risk officers.

Fully integrate cyber risk management into IT disciplines – design for Six Sigma, not quality control. Integrate current technologies to address the latest threats

Execute on strategy

Manage and report on risks

IT DOMAINS

Architecture & Engineering

Infrastructure

Application Development

Security Operations

Other functions…

Copyright © 2015 Deloitte Development LLC. All rights reserved.

The cyber risk program as the "seatbelt" for business innovation

Traditional threats remain, but as the aviation industry reaps the rewards of technology innovation, the industry must also respond to an emerging and ever-evolving array of cyber risks. The consequences are no longer limited to data privacy breaches and compliance penalties. In the worst cases, cyber risks can threaten passenger safety and ultimately the viability of the organization itself. While cybersecurity is viewed by many as a 'necessary evil' that slows down progress, it does not have to be that way.

A seatbelt analogy is apt: the seatbelt provides an additional safety layer to enable faster travel. Likewise, investing in a robust cyber risk program enables the business to continue to compete and grow through technology innovation, but also address the associated risks. For aviation companies, where the network now includes planes and the passengers they carry: "Are you really doing enough to protect your network?"

CONTACTS

Guy Langford
Vice Chairman,
U.S. Travel, Hospitality &
Leisure Leader
Deloitte & Touche LLP
(212) 436-3020
glangford@deloitte.com

Vikram Kunchala
Director
Deloitte & Touche LLP
(713) 982-2807
vkunchala@deloitte.com

Edward W. Powers
National Managing Principal
Cyber Risk Services
Deloitte & Touche LLP
(212) 436-5599
epowers@deloitte.com

ACKNOWLEDGEMENTS
The following individuals have contributed to this paper: Matthew Lew, Tim Corder and Beth Ruck.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms,each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this publication contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.