Data Privacy & Cybersecurity in BizAv

Wednesday, November 2, 2016  1:00 pm - 2:00 pm

PRESENTED BY:
Mark Whitson
Statement of Fair Use

These presentation materials contain copyrighted material, the use of which has not been specifically authorized by the copyright owner(s), except where noted. I am making such material available in my effort to advance understanding of issues related to business aviation and cybersecurity. I believe that this constitutes "fair use" of any such copyrighted material as provided in Sec. 107 of the U.S. Copyright Act of 1976, as amended. According to the U.S. Code, Section 107, the material herein is distributed without profit specifically to those attendees of the National Business Aviation Association 2016 Convention who have expressed a prior interest in receiving the included information for research and educational purposes. This presentation also contains materials with are protected by federal trademark rights, the use of which has not been specifically authorized the trademark owner(s), but which are used solely for commentary purposes, such that I believe that such use constitutes "nominative fair use". This presentation is in no way intended to be used for publication, commercial purposes or in connection with advertising any services of any kind. All rights reserved. The views and opinions expressed in this presentation are mine, and do not reflect the views or opinions held by the copyright or trademark owner(s) of the protected materials used herein.
Themes

• Education
• Collaboration
• Application
Outline

• Concepts
• The Connected Aircraft
• Challenges
• Risk Mitigation
Outline

• Concepts
• The Connected Aircraft
• Challenges
• Risk Mitigation
“When I use a word,” Humpty Dumpty said, in rather a scornful tone, “it means just what I choose it to mean—neither more nor less.”

“The question is,” said Alice, “whether you can make words mean so many different things.”

“The question is,” said Humpty Dumpty, “which is to be master—that's all.”

Through the Looking Glass, Lewis Carroll
Concepts

• Privacy
• Cybersecurity
Privacy

- Whose privacy?
- What is private?
- From whom?
- For how long?
Privacy

What is private?

Protected Health Information (PHI), which is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103).
Privacy
What is private?

- Human Resource Information
  - Depending on the employer, there may be federal requirements to hold information
  - Rules concerning disclosure largely governed by state law
Privacy

What is private?

Consumer Information/History may include information related to an individual's purchases, preferences, complaints and even credit.
Privacy

What is private?

Education History relates to an individual’s education, such as transcripts, or training, such as professional certifications.
Privacy

What is private?

Financial Information constitutes a vast category of information that is highly sensitive and highly regulated.
Privacy
What is private?

Identifying information about property ownership may be protected by privacy laws.
Privacy

What is private?

Identifying information of children under the age of 13 is subject to certain requirements.
Privacy

What is private?

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Confidential Information” means any of the following in a Company’s or Information Holder’s care, custody and control or for which a Company or Information Holder is legally responsible:

(1) Information FROM WHICH AN INDIVIDUAL MAY BE UNIQUELY AND RELIABLY IDENTIFIED or contract, including, without limitation, an individuals’ name, address, telephone number, social security number, account relationship[s, account numbers, account balances, account histories and passwords;
Privacy

What is private?

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Confidential Information” means any of the following in a Company’s or Information Holder’s care, custody and control or for which a Company or Information Holder is legally responsible:

(2) Information CONCERNING AN INDIVIDUAL THAT WOULD BE CONSIDERED “NONPUBLIC PERSONAL INFORMATION” within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1338 (as amended) and it implementing regulations;
Privacy

What is private?

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Confidential Information” means any of the following in a Company’s or Information Holder’s care, custody and control or for which a Company or Information Holder is legally responsible:

(3) Information CONCERNING AN INDIVIDUAL THAT WOULD BE CONSIDERED “PROTECTED HEALTH INFORMATION” within [the meaning of the] Health Insurance Portability Act of 1996 (as amended) and its implementing regulations;
Privacy
What is private?

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Confidential Information” means any of the following in a Company’s or Information Holder’s care, custody and control or for which a Company or Information Holder is legally responsible:

(4) **INFORMATION USED FOR AUTHENTICATING CUSTOMERS** for normal business transactions;
Privacy
What is private?

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Confidential Information” means any of the following in a Company’s or Information Holder’s care, custody and control or for which a Company or Information Holder is legally responsible:

(5) Any third party’s trade secrets, data, designs, interpretations, forecasts, formulas, methods, practices, process, records, reports or other item of INFORMATION THAT IS NOT AVAILABLE TO THE GENERAL PUBLIC.
Privacy

What is private?

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Confidential Information” means any of the following in a Company’s or Information Holder’s care, custody and control or for which a Company or Information Holder is legally responsible:

(5) Any third party’s trade secrets, data, designs, interpretations, forecasts, formulas, methods, practices, process, records, reports or other item of information that is not available to the general public.
Concepts

- Privacy
- Cybersecurity
Security

The National Institute of Standards and Technology (or the “NIST”) defines security as:

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should be part of the enterprise’s risk management approach.

NISTIR 7298, Revision 2, “Glossary of Key Information Security Terms”, Kissell, R. Ed.
Considering the definition of "security", how do you build a "secure network"?

That's a rhetorical question...
Security

Let’s consider instead what is NOT “secure”…
Security
One set of definitions…

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Security Failure” means a failure or violation of the security of a Computer System, including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code. “Security Failure” includes any such failure or violation resulting from the theft of a password or access code from an Insured’s premises, the Computer System, or an officer, director or employee of a Company by non-electronic means in direct violation of a Company’s specific written security policies or procedures.
Security

One set of definitions…

From a “Security Failure/Privacy Event Management Insurance” policy from a major insurance carrier –

“Privacy Event” means ANY FAILURE TO PROTECT “CONFIDENTIAL” INFORMATION (whether by “phishing”, other social engineering technique or otherwise), including, without limitation, that which results in an identity theft or other wrongful emulation of the identity of an individual or corporation.
Security

One set of definitions…

From a “Cyber Extortion Insuring Agreement” from a major insurance carrier –

“Security Threat” means any threat or connected series of threat to commit an intentional attack against a Computer System for the purpose of demanding money, securities or other tangible or intangible property of value from an Insured.
Outline

• Concepts
• The Connected Aircraft
• Challenges
• Risk Mitigation

Sources: enter sources here
The Connected Aircraft
The Connected Aircraft

Walter Beech and navigator Brice Goldsborough demonstrated the practicability of “blind flight”. Year…?

1926, in their instrumented Beech Travel Air “Special” biplane.
The Connected Aircraft

Common Purposes

- Communication
- Navigation
- Air Traffic Control
- Surveillance
- Maintenance
- Business/Mission
- Entertainment
The Connected Aircraft

Networks

- Radio
- Satellite
- Cellular networks
- Manual, Autonomous and Semi-autonomous
User utilizes the aircraft Wi-Fi to access the internet, via the aircraft router.

Connects to the corporate network:

- May access the corporate network securely via VPN ( ),
  - Using VPN = compliant solution

Satellite networks and airborne internet connections are not any more or less secure than other external access points.
Outline

• Concepts
• The Connected Aircraft
• Challenges
• Risk Mitigation
Challenges

• Threats
• Regulatory exposure
• Risk
Challenges
Where privacy and security concerns meet

- Actual Losses
- Regulatory exposure
- Other…?
Threats

Five Ws

• Who?
• What?
• When?
• Where?
• Why?
Threats

WHAT DOES A HACKER LOOK LIKE?
Threats
Threats
Threats

2016?
Iridium Satellite Hacking - HOPE XI 2016

WANTED BY THE FBI

SUN KAILIANG
Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

GU CHUNHUI
Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Threats

Five Ws

• Individuals, private organizations and state-sponsored actors…
• …are gaining illicit access to computer networks…
• …as often as possible and with rapidly increasing frequency…
• …everywhere that those networks exist…
• …for purposes of profit, espionage and sometimes sheer malice.
Domestic and foreign companies may try to illegally acquire your company's information. Foreign nations that seek to improve their economies and militaries target US technology companies.

Common Tactics:
- Computer hacking (Electronic device hacking)
- A virus connects an electronic device to your system, such as a thumb drive, that adds malware or downloads your information
- Someone hacks into your network via a spear phishing attack
- An unsecured laptop is accessed or stolen
- On-site visits to your company
- Unauthorized photography or computer access
- Unauthorized entry into restricted areas
- Asking questions outside the scope of the visit
- Review of publicly available sources. Are you sharing too much information?
- Obtains your surplus equipment. Thousands of pages of stored information may still reside in the memory of a copier, printer, fax machine, etc.
- Employment solicitation (try to hire a key employee)
- Theft or unauthorized photography of products at trade shows
- Burglary (including copying of restricted documents where the originator stays in-house)
- Competitive diving — finding information in your company's trash
- Joint ventures
- Front companies
- Unofficial requests for information
- Extortion — developing a friendship with an employees with the intention of obtaining restricted data or products. The employee will see someone who appears non-threatening and knowable to you as a front.
- Electronic surveillance (listening devices in your home, cell phone hacking, etc.)

Threat of Intellectual Property Could Result In:
- Lost revenue
- Lost employment
- Damaged reputation
- Health and safety concerns from counterfeit products
- Lost inventory
- Loss of research and development
- Delays or interruption in production

Intelsat alone has seen an increase of 80,000 denial of service attacks per quarter to our customer networks from 2013 to 2014, and these attacks are also increasing in frequency, scale and complexity.

Article: *As satellite-enabled networks deliver critical connectivity around the world, cyber-security must be a priority*, Stephen Spengler, CEO & Thierry Guillemin, CTO, Intelsat, pp. 46-47, GlobalHCT 2015
Risk

Where privacy and security concerns meet

- Third-party loss
- First-party loss
- Regulatory exposure
- Other…?
Third party loss

Claims

Substantive
- Breach of Contract
- Negligence, Negligence Per Se
- Consumer Fraud
- Privacy Claims (incl. Publicity to Private Life (the right to secrecy); Appropriation of Name or Likeness; False Light; Intrusion upon Seclusion (the right to be left alone))

Procedural
- Class Actions
- Derivative Shareholder actions
“For victims reporting a monetary loss to the IC3, the average individual loss is about $6,000,” said Ellen Oliveto, an FBI analyst assigned to the center. “The average loss to BEC victims is $130,000.”
First party loss

According to the Ponemon Institute, the average total cost of a data breach in 2015 (64 U.S. companies participating in the study) was $7.01 million. The average cost for each compromised record was $221.

Regulatory exposure

Whether you lost anything or not…

As of 04 Jan 2016:

“Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information.”

Regulatory exposure
Whether you lost anything or not…
Regulatory exposure
Whether you lost anything or not…

- SSAE 16 SOC 1 Type 2
- ISAE3402 - Financial reporting assurance standards
- FISMA Compliance - Protection of government information, operations and assets against natural or man-made threats (Electronic Government Act of 2002)
- PCI/DSS Compliance - Security for credit, debit, and cash card transactions
- HIPAA Compliance - National Security standards to protect patient data
- CJIS Compliance - Criminal Justice Information System
Regulatory exposure
Aviation Compliance – AC 119

SUBJECT: Airworthiness And Operational Authorization Of Aircraft Network Security Program (ANSP)

- WHY THE NEED FOR AN ANSP? Previous aircraft designs utilized ARINC 429, ARINC 629 or Military Standard (MIL-STD) data buses to connect flight-critical avionics systems. Current designs have adopted several technological advances such as Internet Protocol (IP) connectivity to capitalize on speed and weight savings. This advanced technology can be found not only in new aircraft designs but also in postdelivery modifications.
Outline

• Concepts
• The Connected Aircraft
• Challenges
• Risk Mitigation
Risk Mitigation

Recall our themes…

• Education
• Collaboration
• Application
Risk Mitigation

Education

• For aviation professionals: talk to your IT department, learn about networking
• For IT professionals: talk to your aviation network service providers and avionics technicians, learn about aviation systems
• For risk management professionals: read your cyber policy
• For all concerned: consider AeroIT
Risk Mitigation
Education

iGuardian
The FBI’s Industry-Focused Cyber Intrusion Reporting Platform

https://www.fbi.gov/resources/law-enforcement/iguardian
Risk Mitigation

Education

VERIS

Vocabulary for Event Recording and Incident Sharing

- **Actors**: Whose actions affected the asset?
- **Actions**: What actions affected the asset?
- **Assets**: Which assets were affected?
- **Attributes**: How the asset was affected?

Risk Mitigation Education

Corporate flight departments should become educated on their company’s IT security policies. Note that for some 121 and 135 operations, the FAA requires:

“Operators are required to conduct surveillance of their ANSP (Aircraft Network Security Program) to verify compliance with the program and to identify threats to the overall system. An integral part of this surveillance is to analyze threats and report them in a form and manner consistent with its IT security policies.”

Risk Mitigation

Collaboration

For those same 121 and 135 operations, the also FAA suggests internal collaboration:

“Current operator infrastructure may require adjustment to accommodate management of an ANSP. This adjustment usually necessitates **A CLOSER WORKING RELATIONSHIP BETWEEN AIRCRAFT AVIONICS ENGINEERING AND INFORMATION TECHNOLOGY (IT) SECURITY DEPARTMENTS.**”
Risk Mitigation

Collaboration

• Avionics professionals
• IT professionals
• Aircrew
• IT/Data service providers
• Risk management professionals and insurers
Risk Mitigation

Application: three approaches to an identified risk.

• Accept
• Avoid
• Mitigate
Risk Mitigation: three approaches to an identified risk.

• Accept
• Avoid
• Mitigate

OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...

Someday we hope to have a budget.
Risk Mitigation

Application: three approaches to an identified risk.

- Accept
- Avoid
  - Do not transmit or receive data.
  - Do not store private or sensitive information on any device that connects to the Internet.
- Mitigate
Risk Mitigation

Application: three approaches to an identified risk.

• Accept
• Avoid
• Mitigate – where you’ll spend most of your time addressing cybersecurity concerns.
Mitigation

Areas to explore

• Data Center
• Network provider
• Insurance
• Self-help
Mitigation

How secure is your data center?

• Structurally Sound – is it purpose built (as opposed to being in the spare bathroom of somebody's apartment, for example)? Can it withstand foreseeable environmental hazards (like a flood, a CAT5+ hurricane, an earthquake, etc.)?

• High Availability Power – e.g., redundant electrical systems, extended-run generator capacity, etc.

• Multiple Security Levels - audited, compliant, customizable?

• Broad spectrum of data center services - colocation, cloud services, connectivity, consulting, compliance?

• 100% Uptime – Guaranteed?
Mitigation

How ready is your satcom network provider?

• How secure is the provider’s network from attacks?
• What is the provider’s information assurance plan, and does it include steps for prevention, detection, and network restoration?
• Network availability during breach/attack?
• How do the provider’s security protocols assure only authorized access?
• How does the provider keep current with evolving threats?

Mitigation

Risk shifting – insurance

In the last decade, courts have divided sharply on what makes access unauthorized. … Courts have struggled to interpret authorization because they lack an underlying theory of how to distinguish authorized from unauthorized access. … Judges are unsure of how to apply computer trespass laws because the Internet is young and its trespass norms are unsettled.

But see, Travelers Indemnity v. Portal Healthcare Sols, Case No. 14-1944 (4th. Cir., April 11, 2016) (carrier had duty to defend, but not necessarily pay, a class action claim by patients whose data was allegedly lost by insured.)

Mitigation

Risk shifting – insurance

• Policies are available that can help mitigate first- and third-party losses.
• Underwriters sometimes offer auditing services – learn about your weaknesses from a friendly source before a loss occurs.
• Talk to your broker or risk management professional.
Mitigation

Self-help

- Private Jet
- Private Company
- Private Data Center
- Private POPs
- Private Network
Mitigation

Self-help from other departments

- Information assurance training
- Audits/Cyber hygiene
- Recovery plan
Mitigation
Self-help from the IT Department

• Have you changed the admin password on your router…recently?
• Is your wifi logon password-protected?
• Hide the aircraft router SSID, or make its name non-obvious
• Port blocking – for example, allow email but not web surfing
• Captive portal – manage who can log onto your network via username/password
• DHCP pool – limit the devices that can log on
• Cross train IT professionals in aviation networking (consider AeroIT)
Mitigation

Self-help from the Flight Department

• Train users/crews to turn off (or put in ‘airplane mode’) any devices not in active use
• Know what’s on your network – e.g., MATA app
• Information assurance training
• Cross train aviation professionals in networking/IT practices (consider AeroIT)
In the Office

THE GOLD STANDARD

- Your devices
- Your network
- Your IT Security
- Your compliance policies
- = compliant solution
Outside the Office

"IN THE AIR WI-FI" SCENARIO

- User utilizes the aircraft Wi-Fi to access the internet, via the aircraft router
- Connects to the corporate network
  - May access the corporate network securely via VPN ( )
    - Using VPN = compliant solution

Satellite networks and airborne internet connections are not any more or less secure than other external Wi-Fi access points.
Flight departments working with IT is the first step to bringing a company’s onboard systems in line with its corporate compliance initiatives. The FAA expects it already in air carrier ops:

“This adjustment (to accommodate network security) usually necessitates a closer working relationship between aircraft avionics engineering and information technology (IT) security departments.” FAA AC 119-1.
The aircraft’s onboard network can be made to operate completely within the owner’s ground-based network compliance standards (requires the right mix of hardware and software on both).
QUESTIONS AND COMMENTS
NBAABACE

Business Aviation Convention & Exhibition
November 1-3, 2016
Orlando, FL