



**WELCOME TO  
WALA 2015**

Athens,  
Sept 9<sup>th</sup>-11<sup>th</sup>, 2015

## **INSURANCE COVERAGE AND CYBER SECURITY ISSUES**

**Christopher R. Barth**

**Locke Lord LLP**

**11 September 2015**

# What is Cyber Risk?

- A threat against an electronic asset that causes loss, damage and/or interruption with an adverse impact on the “target”
- Access to and use of personally identifiable information or sensitive business information
- Highly technical industries such as aviation could involve so much more

Host



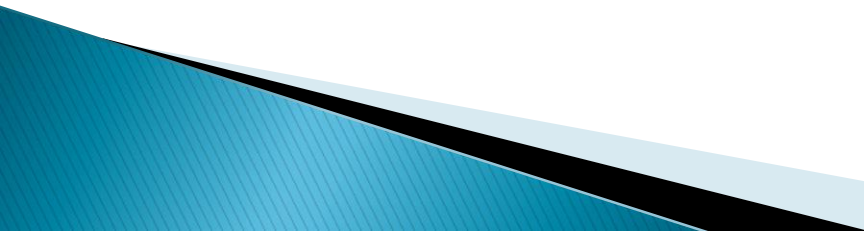
Main Sponsor

**SITA**

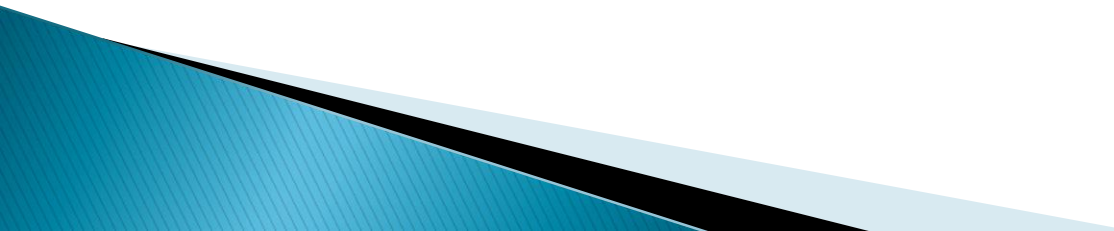
Organized by



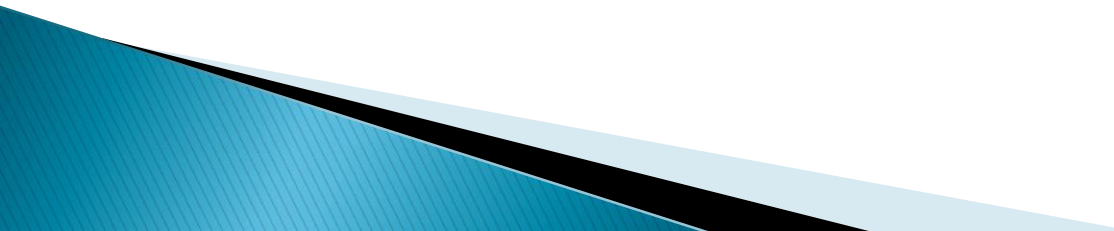
# Examples of Cyber Attacks on Airport / Airlines Operations

- June 2014: Hackers attack ATC systems in Austria, Germany, Slovakia, & Czech Republic
  - April 2015: Hobart AU's website hacked by supporters of ISIS
  - June 2015: United Airline's flights disrupted after hackers entered bogus flight plans in the airline's reservation system
  - June 2015: Operations at Warsaw Chopin Airport disrupted by cyber-attack on LOT Airline's flight - planning computers
- 

# Areas of Risk

- Ground-based computer networks, including ATC systems
  - Interruption of power supplies
  - Attacks on less sophisticated airport service providers
  - Theft of employee credentials, passport photographs, and other secure information to potentially gain access to secure airport areas
- 

# Potential Claims

- Bodily injuries and property damage arising out of system disruptions
  - Personal injury claims for privacy violations
  - Subrogation claims by credit card issuers and their insurers for their response to hacks / breaches
  - Reputational harm
- 

# Is Cyber Risk an “Occurrence”?

- “Occurrence” is typically defined as an accident or exposure to conditions causing damages neither expected nor intended from the standpoint of the insured.
- Scenario: Teenagers hack into Tower ATC, resulting in cancellation of all flights.
- Is it an “Occurrence”?
  - Did teenagers intend to disrupt flights or was that result “accidental”?
  - Claims against airport for failing to maintain adequate security measures?

# Does Cyber Risk Constitute “Personal Injury” Under AVN 60B?

- Standard AVN60 wording: “false arrest or imprisonment, delay, detention, malicious prosecution, wrongful entry to or eviction, from any premises or Aircraft or vehicle or other invasion of the right of private occupancy.”

# Does Cyber Risk Trigger the War Risks Exclusion?

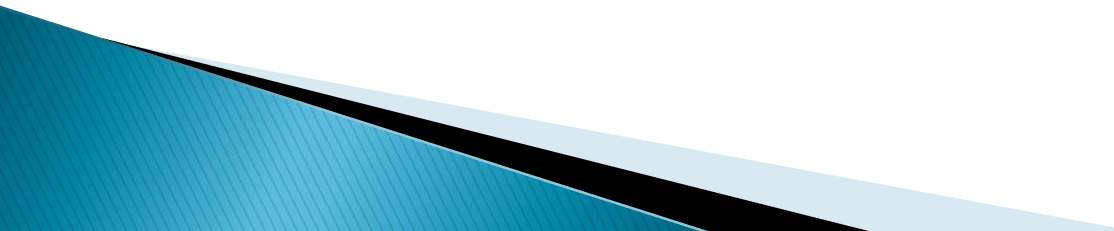
- AVN 48B excludes (in part) claims arising out of:
  - (a) War, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, martial law, military or usurped power or attempts at usurpation of power.
  - (f) Any act of one or more persons, whether or not agents of a sovereign Power, for political or terrorist purposes and whether the loss or damage resulting therefrom is accidental or intentional.
  - (e) Any malicious act or act of sabotage.
- Does an intentional hacking with unintended results fall within AVN48B?
- “Malicious” is defined as “having or showing a desire to cause harm to another person”
- “Sabotage” is “act of destroying or damaging something deliberately so that it does not work correctly”



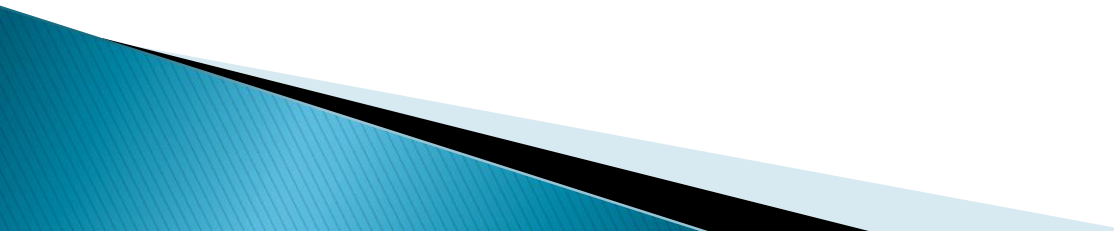
# Control Tower Exclusion

- Some Airport Owners & Operators policies exclude coverage for “bodily injury’ or ‘property damage’ arising out of the direct operation of an air traffic control tower by an insured”
  - Question whether a cyber-attack affecting tower ATC “arises out of the direct operation”

# Cyber Risk Insurance – Specific Cyber Provisions

- “Failure to Follow Minimum Practices” excludes coverage for “any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured’s application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing”
    - Typically based on a misrepresentation in the insurance application
- 

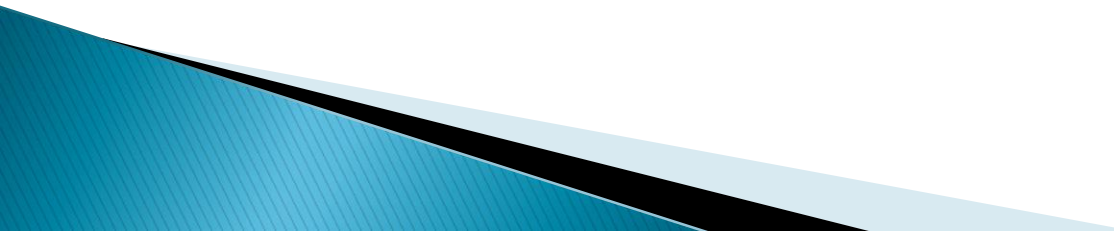
# Cyber Risk Insurance – Specific Cyber Provisions (continued)

- Retroactive dates restricting coverage to breaches or losses occurring after a specific date (e.g. inception date)
  - Exclusion of coverage for unencrypted devices and cloud-based storage
- 

# Cyber Risk Insurance – Specific Cyber Provisions (continued)

- First party coverage to pay for:
  - Forensic examinations
  - Legal counsel to handle breach response
  - Public relations to handle media communications
  - Mailing costs to alert victims
  - Credit monitoring costs
  - Call center staffing
  - Credit card industry fines / penalties
  - Business interruption expenses
  - Restoration of computer systems

# Cyber Risk Insurance – Specific Cyber Provisions (continued)

- Third party coverage for:
    - Defense against lawsuits (especially class actions)
    - Response to regulatory efforts by government agencies and payment of regulatory fines
    - Settlements and damages
- 

# Thank You!

Christopher R. Barth  
Locke Lord LLP  
111 S. Wacker Dr.  
Chicago, IL 60606-4410  
USA

Host



Main Sponsor

**SITA**

Organized by

