LOCKE LORD
LEGAL ISSUE Q&A
Series

Heather Merton
Communications Manager
T: 617-239-0508
heather.merton@lockelord.com
www.lockelord.com

OCTOBER 2015

"Cyber-attacks by their nature are intentional, not accidental, in nature. Such attacks likely do not meet the definition of an 'occurrence' under more 'traditional' policy wordings."

Christopher R. Barth
Partner
Chicago
312-443-0669
cbarth@lockelord.com

Christopher Barth focuses his practice on the areas of aviation and insurance law. In his 20 years of providing legal services, Christopher has defended aviation manufacturers, air carriers and airline consortiums, aircraft leasing companies and lenders, airports and municipalities, charter operators, MROs, and security companies against allegations covering a wide spectrum of issues including wrongful death, product defects, breach of warranty, negligence, faulty workmanship, breach of bailment, and negligent entrustment. Christopher has also handled bodily injury and cargo lawsuits arising under the Warsaw and Montréal Conventions.

Cyber-Attacks on Aviation Industry Rising; Traditional Aviation Insurance Policies Might Not Provide Coverage

Editor's Note: This is one in a continuing series of Q&As with Locke Lord lawyers on key legal issues confronting companies engaged in industries that have national and global impact.

What has prompted an uptick in cyber-attacks on airports and airlines operations?

CB: Cyber-attacks are on the rise worldwide against all industries. The aviation industry – including airports and airlines – are not immune to these intrusions. Hackers likely view the aviation industry as a high-profile target, given the high profile nature of the industry, involvement of aircraft which have the potential to cause significant harm and the heavy reliance on computer systems in all aspects of aviation operations providing many access points to those engaging in such conduct.

What are the areas of risk in the aviation industry?

CB: Those areas which involve the transport of passengers are likely the focus of potential attacks. The 9/11 attacks provide a sad benchmark against which those intending to cause harm measure themselves. Airlines must be particularly vigilant in guarding against such attacks. The next most likely target are those systems with access to financial resources. The vast majority of cyber-attacks are focused on stealing money. The aviation industry involves significant capital resources given the use of such highly complex machinery — e.g. commercial aircraft. The existence of such significant financial resources will attract cyber thieves.

The risk to airport operations tends more towards security aspects. Cyber threats to airports include network intrusions, power supply interruptions and theft of employee credentials and passenger information.

Why do cyber-attacks not fall within traditional aviation insurance policies?

CB: Cyber-attacks by their nature are intentional, not accidental, in nature. Such attacks likely do not meet the definition of an "occurrence" under more "traditional" policy wordings. It is also unlikely that a cyber-attack would result in "personal injury" as that phrase is defined in insurance policy provisions such as the AVN 60 endorsement. Other provisions such as AVN 48B (War Risks) or the Control Tower Exclusion may bar coverage for such claims. The specific facts of each claim must be assessed against an insured's policy wording to assess whether coverage is available under the policy.

What are the specific cyber provisions in cyber risk insurance coverage?

CB: Cyber risk insurance includes many of the terms, conditions, definitions, and exclusions similar to those found in "traditional" aviation policies. In addition, cyber policies include policies specifically addressing technology issues. One such provision is a "Failure to Follow Minimum Practices" exclusion, with bars 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." The provision requires the Insured to continually monitor its systems to ensure it is continually updating its systems, a measure designed to thwart such attacks.

Other provisions include retroactive dates restricting coverage to breaches or losses occurring after a specific date (e.g. inception date) and exclusion of coverage for unencrypted devices and cloud-based storage.