Aviation and airport insurance: Do these specialized insurance policies respond to cyber risks?

By Christopher Barth, Esq.
Locke Lord LLP

Nearly every day the media reports on cyberattacks directed against commercial interests throughout the world. The stakes are massive, as billions of dollars are stolen each year at the "click of a button."[1] No industry is immune to such attacks, and the risks are growing each year as the attacks become more organized and pronounced. A recent report indicates the 2015 average worldwide cost for companies of each such attack is $3.5 million.

The aviation industry is a high-profile target for cyberintrusions. From a financial perspective, aviation — including airport operations, airlines, repair facilities and fueling companies to name a few — involve assets valued in the millions and many times billions of dollars. Aviation operations are technology heavy, relying on computerized systems for virtually every function. These operations present a high-profile target and have been the focus of malicious attacks for decades.

> The aviation industry is a high-profile target for cyberintrusions.

Indeed, as the notoriety to be gained from successfully attacking such targets has been present since the airline hijackings in the 1970s and has continued through the Sept. 11 terrorist attacks. The exposure to passengers and the public in general resulting from such attacks is an ever-present concern and, when coupled with the significant involvement of various forms of technology, represents an added layer of concern.

Media reports on cyberattacks against aviation and airport operations include:

- June 2014: Hackers attack the air traffic control systems in Austria, Germany, Slovakia, and Czech Republic.[2]
- April 2015: In Australia, Hobart International Airport's website is hacked by supporters of the Islamic State group.[3]
- June 2015: United Airlines' flights are disrupted after hackers entered bogus flight plans in the airline's reservation system.[4]
- June 2015: Operations at Warsaw Chopin Airport in Poland are disrupted by cyberattack on LOT Airlines' flight planning computers.[5]

These are the publicly disclosed intrusions, and it is not unreasonable to assume the list is longer. Clearly, hackers recognize various aviation and airport technologies offer an array of targets.

Technologies at risk include:

- Ground-based computer networks, including air traffic control systems.
- Interference with aircraft systems, whether on the ground or potentially in flight.

- Attacks on less sophisticated airport service providers providing a "backdoor" to attacking higher-profile targets.
- Theft of employee credentials, passport photographs and other secure information to potentially gain access to secure airport areas.

From an insurance perspective, cyberattacks on aviation and airport insureds may give rise to claims for bodily or personal injury, and property damage. Policyholders may look to their insurers to respond to claims for:

- Bodily injuries and property damage arising from system disruptions.
- Personal injury claims for privacy violations.
- Subrogation claims by credit card issuers and their insurers for their response to hacks or breaches.
- Reputational harm or business interruption.

In certain respects, traditional aviation and airport insurance tracks the Insurance Services Office Inc.'s general liability policy form. In considering cyber-related claims tendered under these policies, insurers may look to prior court pronouncements involving the ISO policy wordings to assess whether such claims fall within the scope of the more specialized aviation or airport insurance.

One of the first considerations is whether the cyberattack constitutes an "occurrence." Most policies define an "occurrence" to include in part an "accident." Cyberattacks

Christopher Barth, a partner at **Locke Lord LLP** in Chicago, focuses his practice on the areas of aviation and insurance law. In his over 20 years of providing legal services, Barth has defended airports and municipalities, aviation manufacturers, and security companies, among others, against allegations covering issues including premises liability, equipment defects and wrongful death. He is national product liability defense counsel for a European manufacturer of aircraft components. Barth also serves as lead counsel to foreign and domestic insurers in high-exposure, multi-party coverage litigation.

by their nature are intentional, designed to cause harm or to secure ill-gotten gains. One might consider claims arising from these attacks to be outside the parameters of the coverage provided.

However, courts most commonly assess whether the insured was the party committing the intentional conduct; here, it is rare the insured was the actor in committing the attack. In those circumstances where the claims asserted against an insured do not arise from the insured's intentional conduct, the courts may find the claim arose from an "occurrence."[6]

Unlike the question regarding whether cyberattack claims constitute an "occurrence" — a topic for which there is a relative dearth of reported decisions — much of the case law focuses on the results of such attacks.

Specifically, a significant point of contention is in deciding whether the attack resulted in "property damage." Where the attack resulted in physical harm to the computer hardware, the cases have largely found there was "property damage" as that term is defined in the policy.

For example, in *Eyeblaster Inc. v. Federal Insurance Co.,* a widely reported decision, the insured's computers were infected with spyware originating from its website.[7] The question at issue was what constituted "tangible property," a term not defined in the policy. The 8th U.S. Circuit Court of Appeals found the common definition of "tangible property" includes computers, and because the underlying complaint alleged loss of use of computers, the claims constituted "property damage" under the policy. Many other appellate courts have adopted this same view.[8]

Not all courts, however, have adopted the view that "property damage" includes damage to both hardware and software. Those that have not have instead focused on the technical aspects of a computer's operations and how hardware and software are different by their very nature.

In particular, the 4th U.S. Circuit Court of Appeals in *America Online v. St. Paul Mercury Insurance Co.* found the loss of data did not alter a computer's physical functions and, as such, claims arising from purely software issues did not constitute property damage.[9]

As might be expected, aviation and airport operators insurance policies, while incorporating certain common general liability provisions, have their own specialized terms, definitions, exclusions and conditions, some of which might be implicated by cyberclaims.

One such aviation endorsement is the AVN 48 - War, Hi-jacking and Other Perils Exclusion Clause (Aviation)[10] endorsement, which provides in relevant part:

> This policy does not cover claims caused by
>
> * * *
>
> (d) 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.
>
> * * *
>
> (g) Hi-jacking or any unlawful seizure or wrongful exercise of control of the aircraft or crew in flight (including any attempt at such seizure or control) made by any person or persons on board the aircraft acting without the consent of the insured.

Cyberattacks against aviation risks may implicate these particular paragraphs in AVN 48. It is widely known that such attacks are largely done for malicious reasons to inflict harm or secure financial gain through illegal means.

But the risks have gone beyond "typical" hacking events when dealing with the aviation sector. While attempts to gain physical control of commercial aircraft have been virtually eliminated following the Sept. 11 terrorist attacks with the introduction of reinforced cockpit doors, the risks were not entirely eliminated.

In a recent news report, the FBI stated that a passenger, who happened to be a cybersecurity consultant, was able to commandeer an aircraft's engine controls while in flight by hacking the systems over 20 times through the passenger entertainment system.[11] Thankfully, the passenger in question was trying to prove the point that no system is completely secure. Had this been an actual attack resulting in bodily injury or property damage, paragraph (g) to AVN 48 may have excluded coverage for this claim.

Airport insurance policies include their own particularized provisions that address the nature of their operations. An example of specific airport language is in the form of a control tower exclusion. This exclusion commonly provides "[t]his insurance does not apply to ... 'bodily injury' or 'property damage' arising out of the direct operation of an air traffic control tower by an insured."

Traditionally, this exclusion was designed to preclude coverage for claims arising from air traffic controller negligence in the course of conducting tower operations. If a cyberattack results in hackers securing control over the tower's operations, a significant question arises regarding whether this exclusion would bar coverage for bodily injury or property damage claims. Would a court view the commandeering of the tower's controls as a "direct operation"? Is the exclusion limited to the insured's authorized control of the tower so that claims arising from a cyberattack would not be barred? Clearly, claims arising from an attack on a control tower will delve into significant gray coverage areas.

Cyberattacks by their nature are intentional, designed to cause harm or to secure ill-gotten gains.

Aviation policies include an additional area of coverage not found in most general liability policies referred to as "hangarkeepers liability." This coverage is to protect an insured for property damage claims arising from damage to non-owned aircraft in the insured's possession, typically in the course of providing maintenance, repair or overhaul services on non-owned aircraft. The insuring agreement's scope is limited to "physical injury to 'aircraft.'"

Of particular significance in the cyber-risk realm, the typical hangarkeepers liability insuring agreement includes a relatively limited number of coverage exclusions specific to this coverage. While broader exclusions, such as AVN 48 discussed above, apply across all of a policy's insuring agreements, this specific insuring agreement does not include its own exclusions for "expected or intended injury" or Internet-based risks.

One final distinction of note when comparing aviation policies to general liability wordings

such as the ISO form is in respect to language extending the insuring agreement to include personal injury claims.

One of the most common types of personal injury claims arising from cyber risks involves the theft of personal information, such as credit card or banking account information. Most cases addressing personal injury cyberclaims focus on the Coverage B insuring agreement language in ISO policies.

No reported decisions have addressed such claims under the AVN 60 - Personal Injury Extension[12] endorsement, which appears in most aviation policies. This endorsement's opening paragraph states:

> The insurance provided by this policy extends to indemnify the insured for legal liability for damages awarded to any person arising out of one or more of the following offences committed during the policy period but only where such offences are committed in connection with that part of the insured's aviation operations or interests for which other coverage is granted by the policy.

The Personal Injury Extension's scope is importantly limited to "aviation operations or interests." Thus, a cyberattack in respect of non-aviation operations or interests would not trigger coverage under this endorsement.

At the same time, AVN 60 may not exclude certain Internet-related activities from its scope; the ISO wording has included such a carve-out since Dec. 1, 2001. If an airline's reservation system is hacked and credit card information is stolen and then published on the Internet — or, more specifically, the dark net — and this attack results in passengers asserting personal injury claims against the airline, would such claims trigger AVN 60? One can clearly envision an insured asserting as such, particularly if the "offence" resulting in the personal injury is one of those enumerated in the endorsement.

The most recent decision on this issue found that, without publication of the stolen data, there can be no "personal injury" as that term is commonly defined in insurance policies.[13]

Insurance coverage under aviation and airport policies for cyber-risk claims is an area not yet tested by the courts. While decisions interpreting coverage for such claims under non-aviation general liability policies are instructive, the particularized language in the aviation setting presents questions for which there are not yet clear answers and raise doubts as to whether such rulings can be extended to aviation or airport policies. WJ

NOTES

[1] Allianz Global and Corporate Specialty, A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity, (September 2015), *available at* http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

[2] Josh Layton, *Thirteen planes flying over Europe disappear from radar screens amid hacker fears*, Mirror, June 13, 2014, http://www.mirror.co.uk/news/weird-news/thirteen-planes-flying-over-europe-3690154.

[3] Chloe Booker, *Islamic State message on hacked Hobart Airport website*, Sydney Morning Herald, Apr. 15, 2015, http://www.smh.com.au/national/islamic-state-message-on-hacked-hobart-airport-website-20150412-1mji8s.html.

[4] Kim Zetter, *All U.S. flights grounded over mysterious problem*, Wired, June 2, 2015, http://www.wired.com/2015/06/united-flights-grounded-mysterious-problem/.

[5] Mathew J. Schwartz, *Hack attack grounds airplanes*, Data Breach Today (June 22, 2015), http://www.databreachtoday.co.uk/hack-attack-grounds-airplanes-a-8331.

[6] *See, e.g., Lambrecht & Assocs. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. 2003), *citing Rep. Nat'l Life Ins. Co. v. Heyward*, 536 S.W.2d 549 (Tex. 1976).

[7] *Eyeblaster Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).

[8] *See also Retail Sys. Inc. v. CNA Ins. Co.*, 469 N.W.2d 735 (Minn. Ct. App. 1991), and *Am. Guar. & Liab. Ins. Co. v. Ingram Micro Inc.*, No. 99-cv-185, 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (physical damage is not restricted to harm to computer circuitry but includes the loss of access, loss of use, and loss of functionality.)

[9] *Am. Online v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003) (The tangible property is the computer hardware. As underlying claims related to software issues, the tangible property did not sustain damage.).

[10] *See* Int'l Underwriting Ass'n, http://iuaclauses.co.uk/site/cms/contentDocumentLibraryView.asp?chapter=7.

[11] Evan Perez, *FBI: Hacker claimed to have taken over flight's engine controls*, CNN (May 19, 2015), http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/.

[12] *See* Int'l Underwriting Ass'n, supra note 10.

[13] *Recall Total Info. Mgmt. v. Fed. Ins. Co.*, 83 A.3d 664 (Conn. App. Ct. 2014), *aff'd*, 317 Conn. 46 (2015). *See also Zurich Am. Ins. Co. v. Sony Corp.*, No. 651982/2011, *order issued* (N.Y. Sup. Ct. Feb. 21, 2014) (no coverage where the "publication" by the insured, but instead was the result of a criminal act of a third-party hacker).