Fox Rothschild LLP
ATTORNEYS AT LAW

Cybersecurity in the Aviation Industry

Presented by:

Morgan Campbell
Partner, Aviation Group
202.696.1472
mcampbell@foxrothschild.com

Mark McKinnon
Partner, Aviation Group
202.794.1214
mmckinnon@foxrothschild.com

Kristen Broz
Partner, Privacy & Data Security
202.794.1220
kbroz@foxrothschild

U.S.

Atlanta Hit With Cyberattack

City airport cuts off wi-fi as a precaution

TRAVEL NEWS

'Malicious cyber attack' leaves airline to cancel flights in Alaska amid peak holiday travel

Associated Press

Published 2:03 p.m. ET Dec. 22, 2019

Israeli airports fend off 3 million attempted attacks a day, cyber head says

A 24/7 security operation center at Ben Gurion international airport handles cybersecurity threats

By SHOSHANNA SOLOMON

12 February 2019, 2:52 pm

Air Canada app data breach involves passport numbers

29 August 2018

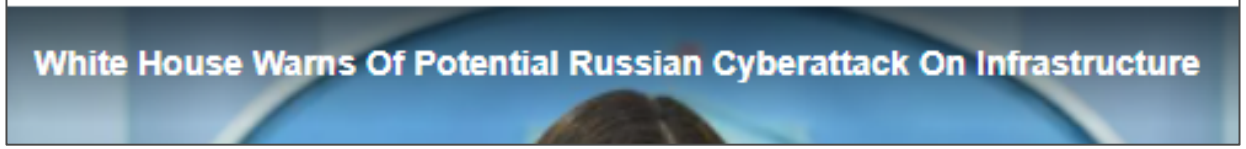
Warning over mysterious hackers that have been targeting aerospace and defence industries for years

Cybersecurity researchers detail a hacking operation that has been conducting phishing campaigns and malware attacks since 2017, despite barely changing its tactics.

NEWS

U.S. Airport Hit With Cyberattack Over Ukraine: 'No One Is Afraid of You'

BY ZOE STROZEWSKI ON 3/29/22 AT 9:16 AM EDT



ANALYSIS | July 24, 2019 | updated 30 Jan 2020 7:26am

Five times airports were involved in cyberattacks and data breaches

As airports increasingly use digital technology in their day-to-day operations they are becoming more vulnerable to attack and data breaches. We take a look at five times airports and airline data became compromised, putting thousands of passengers at risk.

Airlines warn passengers of data breach after aviation tech supplier is hit by cyberattack

Sita, which provides IT of services to 90% of the world's airlines, warns of "data security incident" after falling victim to a "highly sophisticated attack"

Cathay Pacific faces probe over massive data breach

By Reuters Staff

3 MIN READ

HONG KONG (Reuters) - Hong Kong's privacy commissioner will launch a compliance investigation into Cathay Pacific Airways 0293.HK over a data breach involving 9.4 million passengers, saying the carrier may have violated privacy rules.

Importance of Protecting Information

- Legal compliance
- Regulatory compliance
- Effect on brand
- Vendors/partners (commercial litigation)
- Passenger information (class action lawsuits)
- Loss of proprietary information
- Employee information

How They Get In

- Phishing / Smishing / QR Codes
- ID theft
- Hardware theft
- Poor password protection
- Poor patching
- Vendors get phished and pass it on
- RDP vulnerabilities

What They Do Once They're In

- Malware
  - Ransomware
  - Viruses
  - Worms
  - Trojans
  - Bots or botnets
  - Adware
  - Spyware

Harms of Ransomware Attacks

- Encrypted data renders it inaccessible
- Backups corrupted or destroyed
- Anti-virus disabled
- Threats to exfiltrate and leak data
- Double and triple ransoms
- Payment of Ransom but data still inaccessible

Aviation Specific Risks

- Criminal Hacking Group targets aviation and aerospace companies since 2017 (Source: ZD Net – Danny Palmer)
- Hundreds of organizations hit
- Phishing (trying to create urgency) – emails resembling requests for airframe parts or for air ambulance flight details)
- Microsoft Word attachments, Google Drive URL, Microsoft OneDrive URL
- Remote access trojans distributed (the malware can be downloaded from open-source repositories)

Preparing for an Attack or Other Cybersecurity Incident

- Determine location of sensitive data
  - PII
  - Intellectual property
- Assess network security
  - Regularly scan for vulnerabilities
- Monitor network activity
- Restrict access to sensitive data
  - Least privilege principle
  - Need to know

Preparing for an Attack or Other Cybersecurity Incident

- Employee awareness and training
  - Weakest link
  - Challenging in remote environment
  - Leadership buy-in (and leadership training)
- Incident Response Plan / Table-Tops / Audits
  - Outside counsel
  - Business continuity plan
- Multi-Factor Authentication
- Ensure strong Remote Desktop Protocol

Preparing for an Attack or Other Cybersecurity Incident

- Document retention / backups
  - Include protocols for automated data destruction
- Patching / Antivirus / Cloud solutions
- Vendor security management
  - Third party vendors often source of major breaches
  - Security expectations must be built into agreements
- After-Action analysis and lessons learned

Remote Working Risks

- Ransomware attacks spiked during the Covid-19 pandemic
- Increased phishing
- Non-secure employer provided solutions
- Compromised, lost and stolen personal devices
- Unsecure home (or other remote) networks
- Amazon Echo / Alexa

Risk Management and Insurance

- 42% of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages resulting from a ransomware attack (Cybereason, 2021)
- 53% stated their brands were damaged as a result (Cybereason, 2021)
- According to recent GAO report, determining what's covered can be hard for clients because key terms like "cyberterrorism" don’t have standard definitions
- GAO report also noted that the annual global economic cost of cyber incidents may be almost twice the average annual amount of natural disaster losses

Dealing with FAA/Gov't Post Breach

- Regulatory concerns / voluntary disclosures
- FBI Role
- TSA
- DOJ
- Cybersecurity and Infrastructure Security Agency

Dealing with FAA/Gov't Post Breach

- Defense Federal Acquisition Regulation Supplement (DFARS)
  - Controlled unclassified information (CUI)
  - 72-hour incident reporting requirement
- CMMC 2.0
  - Upcoming heightened requirements for defense contractors handling CUI

Data Privacy Laws

- What can you collect and share about your customers?
  - Disclosures to customers
  - Applicable law
- What information must be protected?
  - PII
  - Health information
  - Financial information
- What information must be deleted?
- Do the states in which you operate have differing requirements for data protection and sharing?

Data Privacy Laws

- What law applies:
  - Where the data is stored?
  - Where it is accessed?
  - Where it is used?
- Are you using a cloud services provider to collect and maintain PII?
  - SLA negotiations
  - Incident response
  - International subcontractors
- Is your business subject to foreign laws?

Notifications and Compliance Issues

- Maintain a policy that comports with industry best practices
- Legal requirements will vary depending on jurisdiction
- Notification of individual whose personal information was compromised
- Can notification be delayed based on law enforcement action, and for how long?
  - Key is “reasonableness” in most jurisdictions
- How can the notice be given
  - Electronic
  - In writing
  - Certified mail
  - Phone
  - Are multiple methods required simultaneously?
- Requirements for record retention related to the breach

Notification and Compliance Issues

- Information included in the notice to the victim will vary by state and may include:
  - Type of data accessed
  - Date and duration of the breach
  - 800 number or other means to contact you
  - Description of the breach incident
  - Steps taken to protect the victim
  - Reminder to be vigilant for unusual activity
- Based on scope of the breach and location, notification of:
  - State Attorney General
  - Credit reporting agencies
- Is notification to the government required before customer notification?

Responding to a Breach

- Activate Incident Response Plan/Assemble Team
- Contact breach counsel
  - Necessary to protect privilege
- Contact broker/insurer
- Ascertain status of backup data

Responding to a Breach

- Forensic investigation (outside vendor)
  - Hire investigator through attorney
- Contractual notifications
- Victim notifications
- Credit reporting agency notifications
- State regulators

Mitigating Liability

- Containment
  - Isolate affected systems
- Determine cause of the breach
- Examine policies and protocols
- Determine if correction/change is necessary
  - Consider “Zero Trust”
- Offer protection in the event PII compromised
  - i.e. credit monitoring

Reputational Considerations

- Loss of Business
  - Customers willing to move if breach occurs
- Damage to brand (long term)
- Loss of investors
- Decline in stock value (short or long term)
- Public trust

Lessons Learned from Cyberattacks

- Heathrow Airport (employee lost a memory stick containing unencrypted data - Queen's travel routes, passport numbers, personal data of aviation security personnel)
  - **Lack of encryption, physically removing sensitive data from secured system**
- Atlanta Airport – ransomware attack on City of Atlanta resulted in preventative shutting down of airport Wi-Fi service
  - **Brute force attack to gain entry through weak passwords**
- British Airways – hackers stole names and credit card details of hundreds of thousands of passengers
  - **Malicious code on website stripping passenger info and sending it**
- Cathay Pacific – 9.4 million people had information accessed – passport numbers, travel history, email addresses, credit card information
  - **Investigators attributed to multiple causes, lack of screening for a well-known vulnerability, no effective multi-factor authentication, maintaining unencrypted backups, low alertness for risks**

Lessons Learned from Cyberattacks

- Air Canada – Stolen passport numbers
  - **System passwords weak and did not support strong passwords if customers wanted to use them. Immediate action/account locking isolated damage to small number of passengers. Encrypted credit card info not compromised**
- Swissport – IT infrastructure compromised with Ransomware resulting in flight delays
  - **Swissport was able to restore system through use of uncompromised backup data Attackers later threatened to release 1.6T of information they claimed they had taken**
- SITA – attack on Swiss vendor; Singapore Airlines, Finnair, and other airlines that use SITA had passenger information compromised
  - **Third-party Vendor vulnerability can result in compromise of data from multiple airlines**

Thank You

Morgan Campbell
Fox Rothschild LLP

82020 K Street N.W., Suite 500
Washington, DC 20006

mcampbell@foxrothschild.com
Phone: (202) 696-1472

Kristen Broz
Fox Rothschild LLP

82020 K Street N.W., Suite 500
Washington, DC 20006

kbroz@foxrothschild.com
Phone: 202.794.1220

Mark McKinnon
Fox Rothschild LLP

82020 K Street N.W., Suite 500
Washington, DC 20006

mmckinnon@foxrothschild.com
Phone: 202.794.1214