KYND

Cyber risks in the aviation industry

The aviation industry worldwide is taking off in terms of digitisation. However, with this unprecedented and rapid acceleration in connectivity, there comes a huge concern: cyber risks are reaching new altitudes. As the aviation industry continues to deploy an increasing number of emerging technologies, managing cyber risk is becoming more complex. These rapid changes make the sector a hot target for cybercriminals, who rely on human error. The widespread use of these systems can make implementing even basic cybersecurity measures a daunting prospect.

There's also a glaring vulnerability in aviation companies who still use legacy systems. Upgrading to more advanced systems to keep up with the digitising industry is a large cost, and aviation companies don't always consider this cost to be worth it, even if there are significant cyber risks associated with such outdated systems.

Aviation is a globally interconnected sector, meaning that any disruption can have massive consequences on an international scale. Cyberattacks can cause financial and reputational implications, damage to safety, and potentially severe international impact.[1] Since cyber breaches often target data, such an instance in the aviation industry could even disrupt flight paths or cause problems with flight systems, meaning there is tangible risk to the safety of passengers. An airline can also face substantial GDPR fines over a failure to protect the personal and financial details of its customers. These fines can be up to £18 million or 4% of an organisation's annual global turnover - whichever is greater.

Business exposure and implications

Aircraft

The aviation industry relies upon computer-based interconnected systems, such as air navigation systems, aircraft control and communications, flight information systems, and many others that are necessary for the daily running of operations. The number of digitised processes is soaring, which means training employees in the use of these systems. This makes the risk harder to predict, as you can never totally remove human error from the equation. If human error or malware interrupts any of these processes, there is a physical impact on the ability of the plane to take off, and that can cause huge disruption.

Financial fraud

Airlines have access to very sensitive customer data, such as their passport information and their financial details. Stealing this data is a very attractive prospect for cybercriminals targeting the aviation industry, which can include attacks such as email compromise and invoice fraud, or attacking booking systems and loyalty rewards programs, giving access to customers' air miles.

The danger of domain spoofing

The vast majority of customers buy their airline tickets online, as it's easy and convenient. A large percentage of these customers will also use an airline's website, as opposed to a travel website.[2] Cybercriminals exploit this tendency by registering domain names that look really similar to the airline's website, and tricking customers into handing over their personal and financial details.

Supply chain cyber risk

Even with advanced cybersecurity, a large vulnerability is through third-party service providers and suppliers. Since the aviation industry is globally connected through airports, they are especially exposed to threats. Booking systems, for example, are almost all outsourced to one of a few companies. Airlines also often provide remote access to employees of third-party service providers, giving them access to the airline's systems or applications. If these third-party suppliers don't have sufficient cybersecurity measures in place, the airline is also vulnerable to being compromised by a cybercriminal.

Key industry statistics

£20m

is the biggest-to-date fine imposed by the Information Commissioner's Office (ICO) - on British Airways over a data breach in June 2018 that affected more than 400,000 of its customers[3]

1000

was the average number of cyber-attacks directed against airports every month in 2019[4]

£9m

is the total number of customers whose personal and travel information was exposed in a cyber attack suffered by EasyJet in January 2020[5]

£120k

is the fine imposed on Heathrow Airport by ICO in 2018 for serious failings in its data protection practices after an employee lost a USB stick containing confidential information[6]

What types of risks exist?

There is a variety of different threats that the aviation industry could be impacted by, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

KYND

KYND's analysis of key cyber risks of the top* 100 world's largest aerospace companies
*by revenue

Ransomware Risk

78% of companies had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Email Spoofing

97% of companies were vulnerable to having their email addresses spoofed.

Vulnerable Services

78% of companies were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

88% of companies had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

89% of companies had at least one security certificate which had expired, been revoked or distrusted.

Case Study

Type
A large airline company lost hundreds of thousands of customers' sensitive information to a cyber breach.

Scenario
Customers using the airline's website had their credit card details stolen.

Sting
A cybercriminal was able to inject malicious code into the airline's website. While customers were buying their tickets, their payment data was being sent to the cybercriminal at the same time, and the customer wouldn't even notice. This resulted in the theft of data from hundreds of thousands of customers, including their credit card information. This breach was not discovered until two months later, when a third party noticed it.

Investigation
The subsequent investigation revealed that a cybercriminal had stolen login details from an employee of a third-party cargo service provider, who was using remote login access to access the airline's applications while working remotely. Because the remote login system didn't require multi-factor authentication, and anyone could log in using just a username and password, it was much easier for the cybercriminal to infiltrate the network.

Conclusion
A massive penalty was levied, and thousands of customers had to change their credit card details. This resulted in damage to the company's reputation, as well as inconvenience and stress for the customers. In a global sector where the exposure to cyber risk is widespread, even basic security protocols such as multi-factor authentication can prevent a data breach. Implementing these measures doesn't have to involve technical expertise.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch

 broker@kynd.io

 www.kynd.io

References:
[1] https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-scoping-the-challenge-report/, 2019, Atlantic Council
[2] https://www.independent.co.uk/travel/news-and-advice/consumers-prefer-airline-websites-travel-booking-survey-shows-5540262.html, 2011, Independent
[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/, 2020, ICO
[4] https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Aviation-Industry-and-Insurers-Should-Take-Note-Airport-Interfaces-Are-Potentially-Exposed-To-A-Cyber-Attack, 2019, Crowell
[5] https://www.burges-salmon.com/news-and-insight/legal-updates/data-protection/easyjet-suffers-large-scale-data-breach-and-faces-potential-group-litigation/, 2020, Burges Salmon
[6] https://www.telegraph.co.uk/technology/2018/10/08/heathrow-airport-fined-120000-serious-data-breach/, 2018, The Telegraph