SOLUTION BRIEF

proofpoint.

CONFRONTING HEADWINDS

CYBERSECURITY FOR THE AIRLINE INDUSTRY

PRODUCTS

- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense

KEY BENEFITS

- Protect your employees, customers and ecosystem against all types of email fraud
- Gain full visibility and control for all impostor threats
- Understand how your people put your organization at risk
- Provide consistent training worldwide with support for multiple languages
- Change user behaviour to reduce risks from phishing and ransomware attacks

The airline industry is transforming. Customers are demanding a seamless booking, buying and travel experience. This is why airlines are leveraging digitisation and big data to increase efficiency and better serve their customers. But as airline companies like yours grow to connect and engage with customers, it also exposes you to greater security risks.

The airline technology transformation results in significant increases in the bottom line. For example, The European airline industry generated just over $12 billion of operating profits in 2018, which is an average operating margin of 6%. This is excellent by historic standards, since in the 20 years prior to 2014, the average was just over 2%.[1] But these improvements also expand the airline ecosystem threat surface. And these cybersecurity challenges can be broad in scope. What's more, they can have a far-reaching impact on your customers, your business, and your trusted brand.

Your customers increasingly use smartphones and other mobile devices to book flights and other amenities. This means you need to take proactive measures to protect your customers, their data, and your people.

WHY AIRLINES ARE A GROWING TARGET FOR CYBER CRIMINALS

Airlines store vast amounts of personal and sensitive data. For an average transaction, an airline solicits the name, birthdate, email address, home address, passport details, mobile number and payment information (usually credit card details) of a typical traveler. This database of customer information is a treasure trove for cyber criminals. And that can put the confidentiality, integrity and availability of that data at risk.

Attackers may steal data for financial gain. They use stolen information to create fake identities, steal money or launch phishing attacks. And nation state actors may attempt to manipulate data to disrupt services for political reasons. This adversely affects consumers. In some cases, passport information and loyalty frequent flyer accounts are more valuable on the Dark Web than credit card information.[2]

This increase in data value correlates with the increase in the number of attacks the airline industry has faced recently. In 2018 alone, four major global airlines lost the personal records of nearly 12 million people combined. This is the largest exposure to date. In 2017, an airline lost $3.4 million to a single business email compromise (BEC) phishing attack.

[1] https://www.iata.org/publications/economics/Reports/State-airline-industry-Europe-Apr-19.pdf
[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

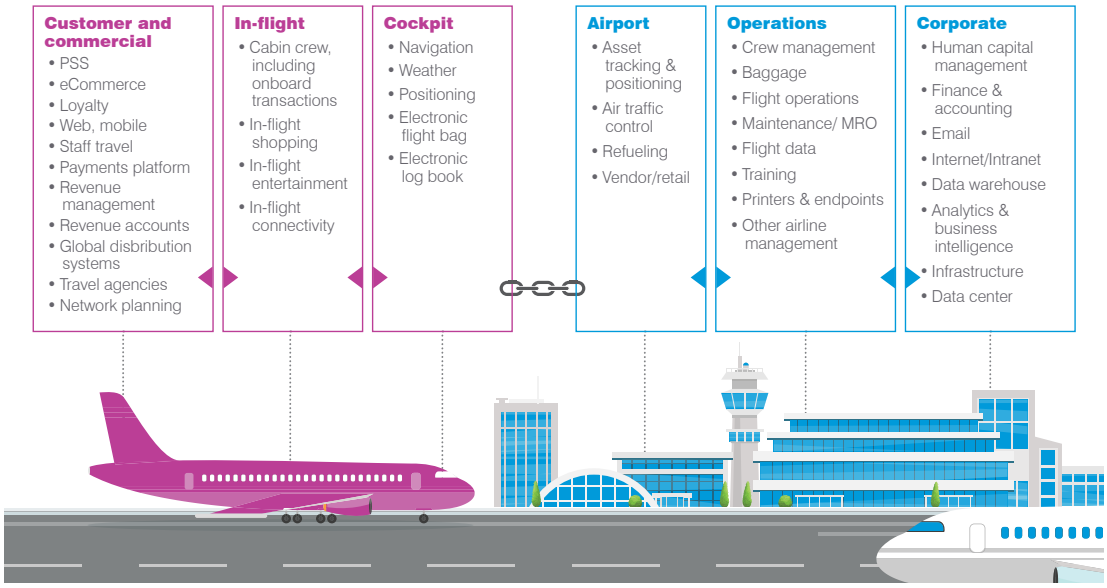
Digitisation Leaves Airlines Open to Fraud

Technology allows for greater connectivity with third-party suppliers. Some airlines have up to 12,000 organisations in their ecosystem. Technology also has increased engagement with customers. At the same time, this digital transformation increases the threat surface in the aviation ecosystem, exposing airlines to increased risk. In its 2018 survey[3] of 59 senior decision makers in the airline industry, SITA found that 83% of aviation organisations include or plan to include cybersecurity in their global risk registers. Ransomware (58%), phishing (52%), and advanced persistent threats (47%) are the top three security risks. Survey respondents say these are their highest priorities.

Proofpoint analysed the domains of 106 European airlines and looked specifically at the implementation of the email authentication protocol Domain-based Message Authentication, Reporting & Conformance (DMARC). DMARC allows airlines to protect their domains from email spoofing, impersonation attacks and other unauthorized use. The results were troubling. Only 18% of the airline domains we analysed—less than 1 in 5—had implemented a DMARC record.

Without a DMARC record in place, your brand can be targeted by cyber criminals. These adversaries can spoof your legitimate sending domains and trick your customers and employees into giving up confidential personal and financial information. Even more troubling, more than 90% of attacks that lead to data breaches target individuals within organisations via email. Airlines are leaving their brands open to being taken over and used by attackers in phishing and fraud campaigns. This puts reputations and customer trust at risk.

Figure 1. Detecting Cyber: The Unique Complexity of an Airline Ecosystem Increases the Importance of an Interconnected Strategy[4]



Airlines Are in the People Business: Trust and Brand Protection Are Paramount

Data breaches and security incidents have an impact on your bottom line. And that impact can be substantial. Cybersecurity has now become a business issue. Breaches can result in regulatory fines. Share prices can drop because of shareholder concerns. And companies can lose revenue when consumers lose trust in their brand and travel with a competitor. Protecting customer data is no longer just about compliance. The goalpost has changed.

IDENTIFY AND PROTECT AGAINST EMAIL FRAUD—PROOFPOINT EMAIL FRAUD DEFENSE

In today's connected world, email is still the main way airlines communicate with customers. Email is used for confirming bookings, sharing boarding passes, or sending marketing promotions. It is also the most vulnerable channel to attacks. With that in mind, airlines cannot rely on customers to spot a fraudulent email. Building a trusted digital business model is vital because trust is reflected in the brand. And that equates to value. Aviation security teams need to ensure that digital

[3] https://www.icao.int/NACC/Documents/Meetings/2018/CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf
[4] https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity-detection.pdf

services and devices can survive attacks.
Proofpoint Email Fraud Defense protects against advanced email threats. This includes email fraud and consumer phishing. When you can see who is sending email from your domains, you can authorise legitimate senders and block fraudulent emails before they reach your employees, your ecosystem, and your customers.

Email Fraud Defense is the only email authentication solution that helps you fully deploy DMARC faster and with less risk.

TEST AND EDUCATE EMPLOYEES TO DETECT AND RESPOND TO THREATS—PROOFPOINT SECURITY AWARENESS TRAINING

According to Proofpoint research,[5] 34% of people around the globe do not know what phishing is. And humans activate more than 99% of today's cyber attacks.[6] That's why 76% of aviation decision makers are now prioritising investment in security awareness and training programmes.[7]

Figure 2. Priorities Investing in Cybersecurity Initiatives

People continue to be the prime target for cyber criminals, so user awareness and education is critical. As threat actors refine their techniques, organisations need to see their users as attackers do. That way, airlines can identify the most at-risk employees. They can base their assessment on targeting frequency and severity of attack. And they can take into account their role, system access and risk exposure.

Engaging airline employees in security awareness training programmes has a proven and measurable impact on reducing their susceptibility to social engineering attacks. Users need to be aware and understand their roles in preventing attacks.

Proofpoint Security Awareness Training can help you understand how vulnerable your people are to a variety of phishing and spear-phishing attacks. CyberStrength®, a powerful web-based knowledge assessment tool, identifies your employees' potential vulnerabilities. And our continuously updated content library provides you with interactive training modules, videos, posters, and images that are translated into more than 35 languages. Also, our PhishAlarm® email client add-on allows your people to report suspicious messages with a single click. And finally, with PhishAlarm Analyzer, the messages your people report are automatically analysed and enriched using multiple Proofpoint Threat Intelligence and reputation systems.

For more information, visit www.proofpoint.com.

[5] https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish
[6] https://enterprise.verizon.com/en-gb/resources/reports/dbir/
[7] https://www.icao.int/NACC/Documents/Meetings/2018/CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf