Maintaining secure, resilient, and safe operations is a top concern for the aviation industry. Digitization and technology provide numerous benefits to aviation but also introduces challenges in addressing cybersecurity flaws. The airline sector offers a prime target for highly motivated cyber adversaries who leverage sophisticated techniques to steal value in money and data, potentially causing harm and disruptions. Also, cyber-attacks and security threats have transnational impacts and components since the global systems are interconnected. The complexity of successful cyber-attacks affects various actors at the international, regional, and national levels. Yet, the civil aviation industry performs its operations in such an insecure environment.

Aviation operations rely on cyber technologies to ensure the efficiency and safety of air travel. Technology dependency and the interconnectivity of critical systems create optimized premises for the emergence of destructive cybersecurity threats. The aviation sector uses multiple interconnected systems for overall operations, including air navigation systems, airport ground systems, on-board aircraft communication, and control systems.

Importance of cybersecurity in the aviation industry

Cybersecurity incidences targeting airports and civil aviation could have caused far-reaching consequences. In 2018, Cathay Pacific Airlines, based in Hong Kong, detected suspicious events in the internal networks. An investigation revealed that cyber actors intruded into the system and unauthorizedly accessed personal data belonging to 9.4 million customers. The accessed data comprised passport information, credit card details, among other types of personal information. The Cathay Pacific data breach remains to be the largest to be recorded in the aviation sector. Subsequently, Cathay Pacific suffered substantial reputational damage, its stock value took a nosedive, and many customers opted for other airlines where their data would be safer.

Also, hacktivist attempts can threaten the trade secrets of the aviation industry. For example, the cybersecurity team of GE Aviation recently worked with the FBI to ward off a state-sponsored attack that attempted to exfiltrate the airline's trade secrets. Had the attack been successful, the trade secrets would have found their way to rival competitors, diminishing GE Aviation's ability to compete globally. As such, the aviation sector must implement sufficient measures to secure customer information and vital trade secrets.
The U.S. Department of Homeland Security (DHS) Secretary, John Kelly, recently announced that terrorists continue increasing their interests in executing attacks to bring down or hijack aircraft following the 9/11 attacks. Kelly also announced a new approach for thwarting such attempts, which emphasized the adoption of new measures that applies across the divide. The proposals include enhanced passenger vetting and increased screening procedures, and challenged the aviation stakeholders to commit to continuous, systematic cybersecurity efforts. Cybersecurity has always been a vital aspect of aviation industry security practices. However, the adoption of newer technologies has made cybersecurity to be crucial to aviation operations.

Best practices for aviation cybersecurity

1. Staff training and evaluation

Many people associate cyber-attacks with savvy and highly skilled hackers. Although this is often the case, studies have shown that approximately 90% of successful attacks and breaches result from human carelessness and errors. The slightest mistakes can expose vital aviation systems to external exploits. For example, losing devices, such as phones and laptops that lack password protection, provides instant access to internal networks. In other cases, employees may furnish hackers with confidential information if they fall for phishing and other social engineering attacks. To mitigate such occurrences, airports, and other businesses in the aviation industry must expose all employees to consistent and frequent training opportunities. Training reduces the possibility of attacks since staff personnel can avoid errors and maintain adequate security hygiene.

2. Active monitoring and data flow mapping

The aviation sector can only detect cyber-attacks and respond effectively by actively investigating and looking for suspicious network and system activities. Monitoring processes begin with updated analysis and evaluation of data flow in a specific area. For accurate and full network mapping, organizations in civil aviation should consider factors, such as the storage location of sensitive information (is it in the cloud, online or onsite servers?), the implemented data backup policies, and individuals with access privileges. Full data flow mapping enables monitoring of the potential access points and accurate logging of user-data interactions. As a result, organizations can easily pin-point attacks and respond appropriately.
3. Risk assessment and prevention

Although there are numerous similarities between the aviation cybersecurity practices and those of other industries, security professionals in aviation experience unique challenges. Innovative and emerging technologies improve communication in airlines but at the cost of new security vulnerabilities. To ensure maximum security, aviation stakeholders require to assess cybersecurity threats of more modern technologies proactively. For example, the Federal Aviation Administration is modernizing its air traffic control systems by upgrading the radar-based systems to GPS-based systems. Although providing many advantages, GPS has internet connectivity capabilities and requires consistent risk assessment and mitigation. A holistic evaluation based on global frameworks and standards can enable risk identification and prevention.

4. Cybersecurity information sharing

Organizations in the aviation industry must frequently share cybersecurity information by following a "learn once, share widely" model. Sharing data, such as threat data, security log events, and thwarted attacks, can promote robust risk management efforts, effective mitigation practices, and increased visibility of security risks. Relevant standards and regulations regarding sharing security information in a responsive and timely manner must be enforced to ensure the aviation sector remains several steps ahead of attackers.

5. Cybersecurity incident management

Despite the measures or controls implemented to protect the aviation sector from cyber-attacks, the industry stakeholders must understand that it is only a matter of when an attack will happen. Therefore, aviation entities must be ready to handle, manage, and prevent cyber incidence from escalating. Incident management requires a collaboration between the staff responsible for securing the aviation products, such as aircraft and operations, and the network operators (CISO). The partnership is essential since it facilitates skills and knowledge sharing to ascertain effective incident management. All involved members should frequently train by simulating attack scenarios, as it guarantees prompt incident management once it occurs. The processes and governance around the organizational structures are vital in ensuring sufficient incident management efforts.