POINT OF VIEW

Airline Cybersecurity Priorities Now and After the Pandemic

Safeguarding an evolving industry

by Ramesh Perumal,
Security Solution Lead, Cyber Security
Prashant Deo,
Security Consultant, Cyber Security
Geetali Raj,
Presales Lead, Cyber Security

Abstract

Nearly every industry has experienced devastation from COVID-19, but only a few have been hit as severely as the airline industry. While rushing to respond to this threat to passenger safety and company revenues, airlines are also aware that any measures taken must not compound existing threats. In particular, one ongoing mandate looms even larger as new business and operating models emerge: cybersecurity.

Near-term or long term, airlines will need to consider the impacts to its security posture at each stage of its response. While the unexpected can and will happen, many security impacts can be proactively mitigated.

Security leaders must be active participants in any new initiatives designed to mitigate the effects of COVID-19 on the business. Cybersecurity, including privacy controls and relevant threat modeling, should be factored into these initiatives from the outset. By treating security measures as a critical element of design rather than an afterthought, the airline industry can more confidently move into its new beginnings.

Slashing costs in the near-term

Recent images of empty terminals and cancelled flights falsely give the impression that the airline industry has ground to a halt. In reality, airlines are working around the clock to provide essential services like transporting goods, patients and healthcare workers. They are providing these services even with their main sources of revenue greatly diminished as a result of near-zero passenger carriage.

The passenger segment may not recover any time soon, given how severely the pandemic has affected business operations, travel and tourism, and economies across the globe. It's widely anticipated airlines will have to reduce the number of seats per plane to enforce social distancing. Fewer available seats will likely lead to higher prices, which could in turn further depress passenger travel. In addition, the airline industry may need to scale down or optimize current routes, as airports will probably operate at suboptimal capacities to save costs.

Additional cost pressures are likely to result in a "make do with less" mindset for the foreseeable future. Outcomes like further resource layoffs and the need to optimize current investments will put added pressure on security leaders. With spending limited to critical business services, they will be expected to cut planned capital expenditures and improve operational efficiencies. Amid such belt-tightening measures, however, some modernization can take place, including switching to consumption-based, "pay-as-you-go" security services, consolidating disparate or redundant solutions, and developing more stringent business justifications for security tools.

New business and operating models

Beyond initial cost-savings measures, newer technology can help airlines become healthier environments for passengers and employees that are both more efficient and more secure. The industry has historically hesitated to make major technology changes quickly — as evidenced by fleets with an average age of 10-20 years and the occasional use of paper tickets that still conform to the dimensions of a punch card. But it has also shown itself able to respond to challenges (such as heightened security measures) and opportunities (such as WiFi) when they present themselves. The current crisis will likely present such a moment for airline companies.

Touchless ground, boarding and onboard operations

Already focused on passenger safety, the aviation industry must also now give priority to ensuring the health of its customers, staff and partners. Touchless user interfaces will form a core part of this strategy, from systems based on radio-frequency identification (RFID), near-field communication (NFC) and infrared (IR) standards to sophisticated facial recognition programs, yet these advanced techniques can bring vulnerabilities of their own.

From the first day of development to deployment and operations, security teams should perform vulnerability tests to ensure the Agile, DevOps and infrastructure environments are secure. These systems may also require exception handling and governance measures to ensure data privacy, user confidentiality and regulatory compliance.

Preventive onboarding measures

There will likely be increased medical devices and healthcare services onboard for managing COVID-19 or coronavirus-like indications, which may require actions performed by staff or other authorized individuals. Airlines will need to verify this information during preboarding and while onboard through multifactor authentication and correlation with records.

As a result, the personal health information (PHI) data of passengers will likely get captured to determine onboarding decisions and potential medical aid interventions. To enable these procedures, security leaders will need to establish data security measures to identify, classify and protect captured PHI data appropriately.

Remote working models

With fewer onsite staff members, more services – such as check-in, verification, passport and visa controls, and retail services – will need to be done remotely as much as possible. Deploying augmented and virtual reality (AR/VR) solutions for interacting and guiding travelers can enable this requirement. In addition to deploying additional security controls in airport spaces, these technologies will also involve remote workspaces for employees that need to be secured with end-point protection as well as the ability to protect data in transit.

And with many support staff operating remotely for an indefinite period, cyber criminals will try to exploit this opportunity to penetrate systems and launch attacks when airline operations are operating at full capacity. It will be critical for security teams to perform quick and frequent threat assessments and breach-and-attack simulations to test for system compromises and vulnerabilities.

Goods and freight

A good portion of the industry's evolution may include transforming passenger airlines and airports into cargo transportation and warehouse operations. All measures that apply to such organizations would also apply to airlines and airports, including surveillance, B2B controls and regulatory compliance.

As new business models and revenue streams come to light, airlines will need to identify and manage security risks for newly emerged supply chain and partner ecosystems. Some of these risks could include collaborating with wholesalers and retailers, pharma companies, oil and gas and other conglomerates as revenue models shift to goods and freight.

Staff and partner enablement

With more focus on goods and medical services across the industry, employees and air traffic controllers (ATCs) must be kept current on the latest government information and regulations. Regular enablement for remote staff and partners must ensure the information reaches the appropriate people with minimal risk of its misuse or modification.

Maintaining more stringent business continuity plans (BCPs) to mitigate widespread impacts from future pandemic situations will also involve ongoing training for employees, ATCs, customers and partner relations staff, regardless of their location.

B2B assurance and engagement models

Aviation is characterized by a high degree of interdependency of multiple players. The industry must rely on the engagement and active participation of regulatory authorities and all of the stakeholders of the travel and transportation ecosystem to ensure a sound, seamless and sustainable recovery.

This principle also applies to the digitization and automation of processes to increase operational efficiency and provide security. Many airlines are adopting blockchain to track cargo and baggage, manage passenger identities and execute agreements embedded into code as "smart contracts." While a boon to enabling trust and efficiency, the applications involved in these exchanges and recording keeping must themselves must be made secure.

Declarations and compliances

As the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA) assess their requirements for ensuring the health and safety of their staff and passengers, airlines and airport security operations may need to meet increased or changing regulations and guidelines. Travelers may need to fill out more declarations (with more personal information than before) before takeoff or before arriving at their destinations to establish their ability to travel and to enable contact tracing. Only by prioritizing data security, data privacy and user confidentiality can airlines and airports maintain consumers' trust and achieve truthful compliance.

Crowdsourcing, collaboration and M&As

While the airline industry struggles with leaner staff, less capacity and falling revenues, there will likely be an increasing need to collaborate with other players in the industry to help drive down costs and improve efficiencies. Airlines may decide to crowdsource operations like predictive aircraft maintenance, fuel optimization and traveler systems, for example. And the probability of significant merger and acquisition activity will likely only increase at all levels, as survival plans, new growth strategies and market retention efforts take shape.

As with any new configuration of companies working with or becoming part of other companies, cybersecurity protocols and platforms need to be standardized across participants. Defaulting to the most up-to-date and flexible option among redundant or competing security platforms and services often makes the most immediate sense. However, considerations for future growth and freedom of movement may argue for wholly new service providers and capabilities for all involved. Keeping one eye on future collaboration and innovation needs while ensuring cybersecurity defenses remain equal to emerging

threats and risk exposures should be the concern of Chief Information Security Officers as well as other C-suite and line-of-business leaders.

Moving forward in a post-COVID-19 era

Throughout the initial cost-cutting period, security leaders will face a delicate balance of optimizing cybersecurity spending weighed against risk exposure. They will need to use innovative methods to maximize defenses and adapt to the new normal. Once the situation normalizes and as the industry ventures into new business models, security leaders will need to shift their focus to ensure cybersecurity is incorporated from the outset of corporate initiatives.

Time and time again, the airline industry has proven its resilience. By making cybersecurity a priority throughout their business model transformations, airlines can once again prevail in a post-COVID-19 era.

TATA CONSULTANCY SERVICES

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty.

IT Services
Business Solutions
Consulting

Corporate Marketing | Design Services | M | 06 | 20