CYBERSECURITY RISK MANAGEMENT

Risky altitudes: The cybersecurity state of airlines

Executive summary

Air travel is a key component to the global economy, moving people and goods around the world every single day.

To keep this vital industry moving airlines work with and rely on, hundreds of third-party service providers from security personnel, ground operations, baggage handlers, payments provider and customer support. Any form of disruption to this intricate digital network can prove disastrous for both the airlines and their customers which is why it is vital for them to know how secure their digital ecosystem is, and where the cybersecurity weaknesses within their network of third-party vendors may be.

This report focuses on the cybersecurity posture of the top 20 airlines - based on flight frequency (volume) and the top 20 airports – based on number of seats sold (capacity) and their supply chain digital footprints. This analysis was completed utilizing RiskRecon by Mastercard to evaluate the cybersecurity of the top 20 airlines and top 20 airports, their supply chains and their third-party vendors. This report explores commonalities visible within the industry and highlights areas of concern, with the ultimate purpose of raising awareness for the airline and transportation sector on where they can improve their cybersecurity posture.

Key findings

7.5 out of 10 (B rating) - the average cyber risk rating of top 20 sampled airlines.

80% - (16) of the sampled airlines had an overall risk rating of an A or B, indicating their information security programs may be sufficient to protect their data assets.

20% - (4) of the sample airlines have a rating at or below a C, indicating that there may be security gaps present in systems that could potentially result in data compromise.

In comparison;

7.3 out of 10 (B rating) - the average overall risk rating for the whole Transportation and Warehousing sector

Introduction

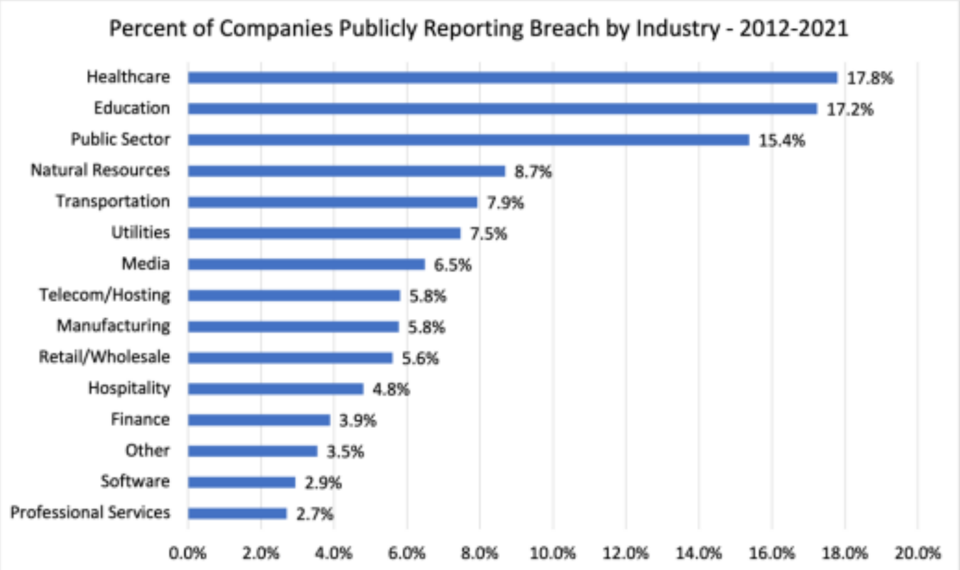
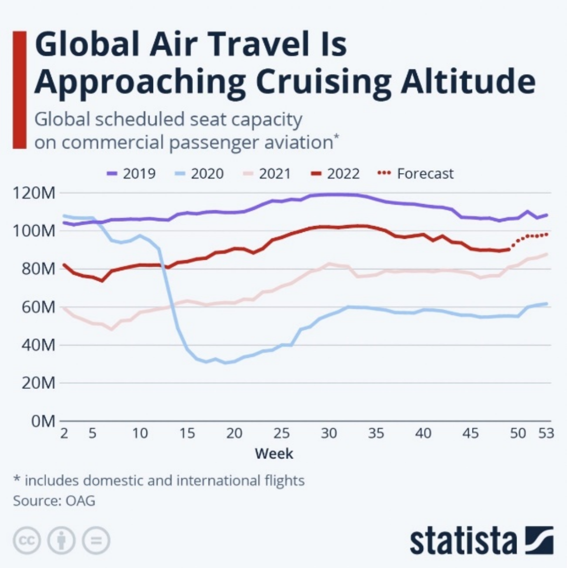


Figure 1[3]

Airlines handle copious amounts of personal identifiable information (PII) everyday which includes passenger's passport details and card payment information. A RiskRecon by Mastercard study found that between 2012 and 2021, the Transportation industry was in the top five for sectors in publicly reported breaches.[1] With travel resuming post COVID-19 and an estimated seven billion passengers flying in 2022[2], airlines may find themselves becoming prime targets for cybercriminals globally.



* includes domestic and international flights
Source: OAG

Figure 2[4]

This report focuses on the current cybersecurity posture of top airlines and airports by utilizing RiskRecon, Mastercard's third-party risk monitoring capability, to evaluate their digital footprints. It explores commonalities visible within the industry and highlights areas of concern, with the ultimate purpose of raising awareness for the airline and transportation sector on where they can improve their cybersecurity posture. The top 20 airlines included in the sample performed relatively well with an average B (7.5) in the overall RiskRecon risk score. This was on par with the average overall risk rating for the whole Transportation and Warehousing sector with a B (7.3). While this is promising to see, there is still areas of weakness that could be strengthened to assist in bringing down overall risk.
The COVID-19 pandemic devasted the aviation industry resulting in over US$160 billion in economic losses in 2020[3]. Air travel did not truly begin recovering until 2022 once restrictions

[1] RiskRecon - Paper: Risk Management Insights from 10 Years of Data Breach Events (riskrecon.com)
[2] CAPA – ACI World - global passenger traffic up by 53% in 2022; movements by 20%; cargo down | CAPA (centreforaviation.com)
[3] McKinsey & Company - COVID-19's impact on the global aviation sector | McKinsey

lessened and the pandemic started subsiding.[4] Following this two-year lull, airlines started operating again in earnest which made them a prime target for cyber threat actors. This is reflected within the sample for this analysis where 45% of the organizations disclosed 12 data breaches in total since 2020. 75% of the breach disclosures during that period were due to third-party services used by the airlines, six of those disclosures being from a single breach event[5].

Airlines work with a myriad of third-party service providers from security, ground operations, customer support, and more to move billions of people annually. Due to the hundreds of third-party service providers that help airlines operate, this report evaluates the top airports, specifically evaluating the top 20 airports. If even one of these airports is successfully attacked, millions of passengers could be affected. This is such a large concern that the Australian government ran a mock cyberattack scenario at the Sydney Airport in July 2023[6] where officials from the Department of Home Affairs, the Australian Cyber Security Centre, representatives from the Sydney airport, and others were present to establish and practice procedures following a cyberattack.

With increased targeting, governments globally are taking measures in a multitude of ways to better secure airline-related critical infrastructure. In March 2023, the United States Transportation Security Agency (TSA) issued a new cybersecurity amendment requiring "impacted TSA-regulated entities develop an approved implementation plan that describes measures they are taking to improve their cybersecurity resilience and prevent disruption and degradation to their infrastructure" along with other measures outlined by the TSA[7]. The European Union Aviation Safety Agency (EASA) published *Commission Implementing Regulation (EU) 2023/203* in February 2023 which "lays down rules for the identification and management of information security risks in aviation organizations and aviation competent authorities"[8].

[4] World Economic Forum - This chart shows how global air travel is faring post COVID | World Economic Forum (weforum.org)

[5] RiskRecon data pulled as of August 15, 2023

[6] The Sydney Morning Herald - Cybersecurity: The 'nightmare' scenario being war gamed by government (smh.com.au)

[7] TSA - TSA issues new cybersecurity requirements for airport and aircraft operators | Transportation Security Administration

[8] EASA - Commission Implementing Regulation (EU) 2023/203 - Requirements for the management of information security risks with a potential impact on aviation safety for organisations and competent authorities | EASA (europa.eu)

RiskRecon by Mastercard overview

What is RiskRecon by Mastercard?

RiskRecon is Mastercard's third-party risk monitoring capability that assesses and scores the cybersecurity performance of an organization using open-source intelligence. RiskRecon employs passive, non-invasive techniques to discover an organization's public systems and analyze those systems' cybersecurity risk posture. RiskRecon summarizes organizational results in an easy-to-understand score called a RiskRecon Cyber Risk Rating, which provides a rapid orientation of the organization's cybersecurity performance.

RiskRecon Cyber Risk Rating

RiskRecon's Cyber Risk Rating is an overall security rating based on performance across 9 Security Domains. The rating scale is A – F, with A being the highest possible positive score. The Security Domains measured are software patching, application security, web encryption, network filtering, breach events, system reputation, e-mail security, DNS security, and system hosting. For further detailed descriptions of the 9 Security Domains, please refer to Appendix A.

Asset Values and Priority

RiskRecon determines the value at risk (asset value) of a system based on deep analytics of the code, content, and configuration of each Internet-facing system. Through these analytics, RiskRecon discovers the types of data each system collects. The primary analytics are focused on identifying the form fields of every web page and using machine learning models to determine the types of data each collects. Systems that collect sensitive data such as user credentials, email addresses, credit card numbers, and so forth are rating as High asset value. Systems that collect no sensitive information are given a lower rating. RiskRecon combines issues and their priority with the asset value information to get a fuller picture to assess overall risk.

Security Issues

RiskRecon automatically contextualizes every issue with severity and asset value, enabling information security professionals to easily identify risk priorities and needed action. The highest priority findings are issues that are considered critical severity (based on Common Vulnerability Scoring System) discovered on high-valued assets (e.g., a system that collects login information or Personally Identifiable Information).

Methodology

The sample used in the airlines analysis[9] consists of 20 airlines which were based on statistics published by OAG[10], a data platform for the global travel industry. OAG identified the top 20 airlines globally with the largest volume of flights scheduled in July 2023.

Disclaimer: The purpose of this report is to raise awareness about the visible risks and vulnerabilities amongst airlines and airports by illustrating the current cyber risk landscape of the airline industry in the context of other industries and geographies. It is not to cast blame or examine the root causes of the current cyber posture of airlines.

Sample selection methodology

The sample used in the airlines analysis[11] consists of 20 airlines which were based on statistics published by OAG[12], a data platform for the global travel industry. OAG identified the top 20 airlines globally with the largest volume of flights scheduled in July 2023.

It should be noted that all airlines in the sample were evaluated as individual entities and not at the parent level. For example, subsidiaries of International Airlines Group (IAG) include Aer Lingus, British Airways, and Iberia. If we wanted to evaluate Aer Lingus, *which is not part of our sample*, we would analyze only Aer Lingus' digital footprint and assets rather than evaluating at the parent level which would include the digital footprint and assets of all IAG's subsidiaries.

The analysis[13] of airports consists of the top nineteen airports globally based on the number of seats sold in August 2023. The statistics published by OAG[12] included the top 20 airports but the domain for one airport was unreachable[14], and therefore was excluded from this analysis.

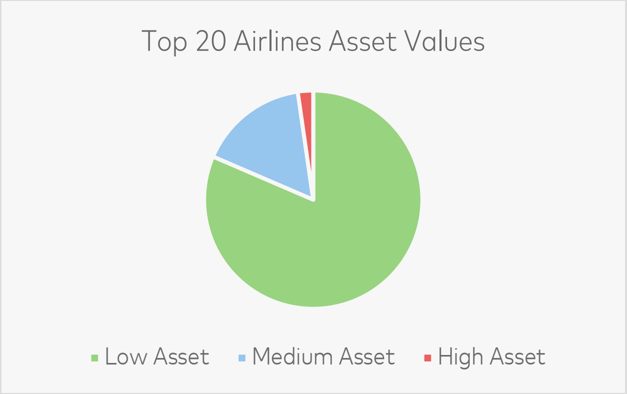
Sample makeup

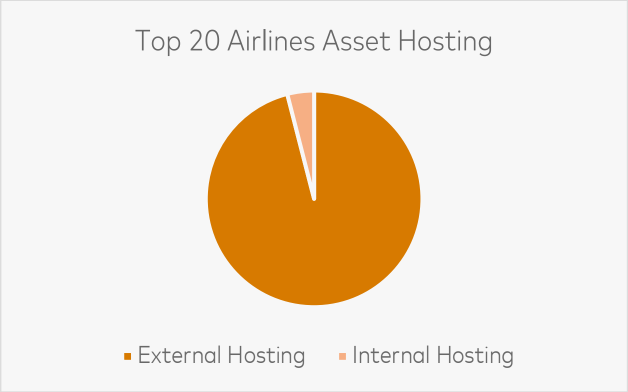
RiskRecon maintains a continuous inventory of the enterprise internet surface, discovering systems using supervised machine learning algorithms that mine enterprise systems from the internet through examination of data collected from analysis of global domain and netblock registration databases, internet crawling, and subsidiary analytics. RiskRecon system ownership attribution is independently certified at 99.1% accuracy. Based on this technology, RiskRecon enumerated the digital IT footprint of the airline sample set. The sample is composed of airlines that are headquartered around the world and vary in digital portfolio size[15]. The median number of hosts

[9] RiskRecon data pulled on August 15, 2023
[10] OAG - Airline Frequency & Capacity Trends Statistics | OAG
[11] RiskRecon data pulled on August 15, 2023
[12] OAG - Airline Frequency & Capacity Trends Statistics | OAG
[13] RiskRecon data pulled on September 13, 2023
[14] The site was unreachable as of September 12, 2023
[15] RiskRecon data pulled on August 31, 2023

registered is 510 and those are, on average, hosted across eight countries by 33 service providers per airline. 96% of hosting for the sample is external and the majority (81%) of all assets, hosted internally and externally, are classified as "low value" by RiskRecon. The number of domains varied widely, with an average of 400 domains per airline.

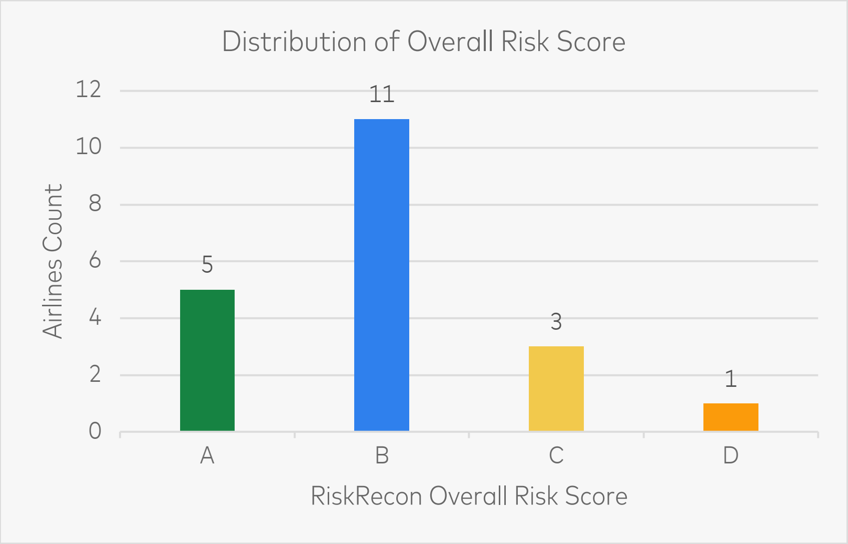
Findings





Overall, the 20 sample airlines performed well with an average RiskRecon overall risk rating of **B (7.5)** rating. 80% (16) of the airlines had an overall risk rating of an A or B. An A or B rating indicates that an organization seems to have sufficient security programs in place to protect their assets. On the other hand, 20% (4) of the sample airlines have a rating at or below a C, indicating the likely presence of significant security gaps that could lead to data and system compromises. The lowest scoring airline had 25% of the total disclosed breaches since 2020, where 2 out of the 3 disclosures were due to a breach of a third-party provider.

RiskRecon classifies organizations into larger industry groups, airlines falling within the Transportation sector. The top 20 airlines in the sample performed on par with the transportation industry's overall rating, B (7.3).



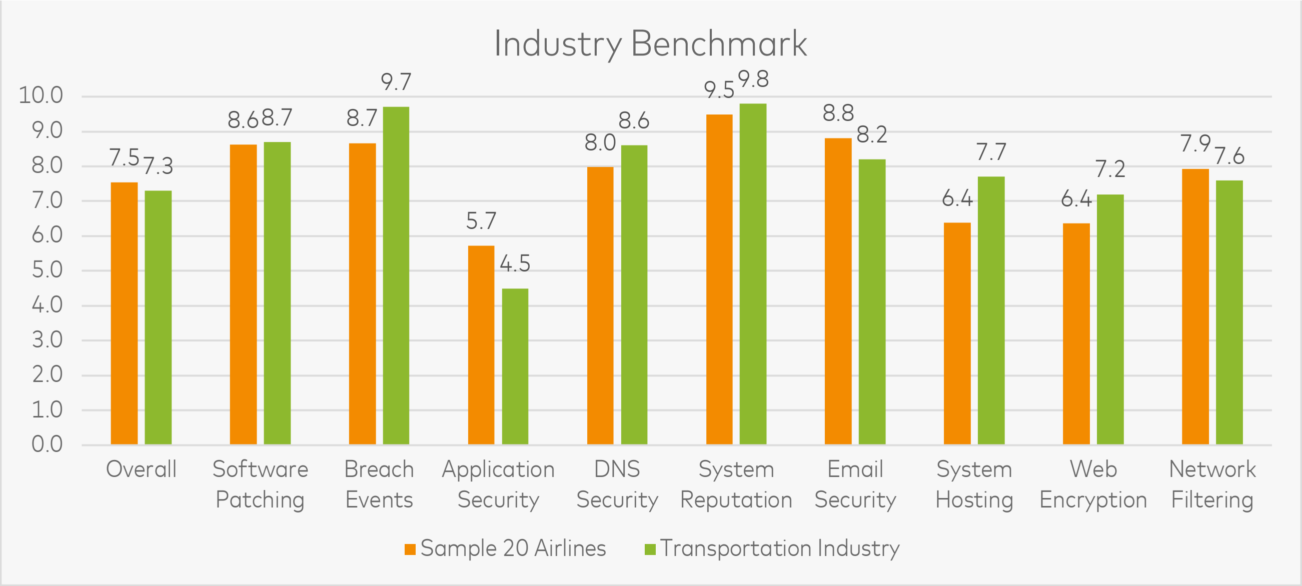


Figure 3[16]

The chart above provides further details of the airlines' and transportation industry's performance across RiskRecon's nine security domains. The transportation industry outperformed the airlines in six of the nine security domains. The industry performed especially well in System Reputation and Breach Events and scores poorly in the Application Security domain. Despite nearly half the sample airlines experiencing at least one data breach in the last three years, it can be observed that airlines still performed well on average in the Breach Events domain with an 8.7 (A) rating.

Security issues and trends

RiskRecon enables organizations to monitor their cybersecurity risks through open-source intelligence techniques. In addition to the alpha-numeric ratings, RiskRecon also identifies specific security issues. These issues are prioritized based on issue severity and asset value. The most severe issues found on the most valuable assets are categorized as the highest priority issues in RiskRecon. For more details about how RiskRecon prioritizes issues for customers, please refer to Appendix B.

The 20 sample airlines had a total of 218,483 security findings though only 37 (0.02%) security findings were classified with the highest priority. It can be noted that 90% of the findings belong to airlines with a C or below overall risk rating. This is a promising statistic since only four of the sample airlines fall at or below the C rating and could make significant strides to remediate security issues.

[16] Data for Transportation Industry averages pulled as of September 5, 2023, including data for over 1000 transportation entities. Data for Top 20 Airlines averages pulled as of August 15, 2023.

Of the nine RiskRecon security domains, the graph in Figure 4 shows that almost all findings are tied to Application Security, System Hosting, and Web Encryption with the remaining six Security Domains accounting for a combined 1,345 findings. Below, there is a deep dive going into key security issues and trends including Application Security, Web Encryption, Software Patching, and Social Engineering. While the former two make up the bulk of the security findings, the latter present some of the largest risk where lack of awareness and education, could lead to detrimental results.

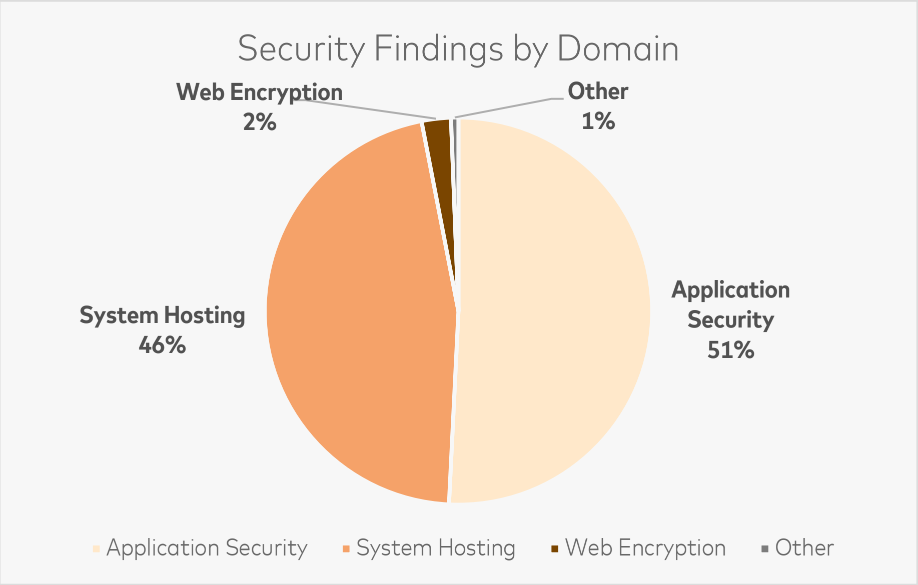


Figure 4

Security Issue – Application Security

RiskRecon assess websites for the presence of five important HTTP security headers within the Application Security domain which provide instructions to the browser for secure interactions. Without these security headers in place, it gives attackers easy infiltration points to collect sensitive data or inject malicious code into requests. The Application Security domain had the lowest average score of a D (5.7) out of all security domains and 100% of all entities in the sample had at least one missing HTTP Security Header. Cross-site scripting (XSS) is a common attack that can be executed with missing HTTP Headers, allowing remote commands on web browsers which could result in the stealing of login credentials, payment information, and other personal details. It can be noted that missing HTTP security headers is a prevalent issue across many industries that RiskRecon evaluates.

Security Issue – Web Encryption

Despite the Web Encryption Security Domain only accounting for 3% of total findings, there is impact seen across all 20 sampled airlines. The two main issues within the security domain were expired certificates and invalid certificate subjects which affect how users interpret the security of websites they visit. Expired encryption certificates are invalid, causing the browser to display security warnings to users and preventing users from easily validating the authenticity of the site and systems with an invalid certificate subject are not trustworthy and cause the browser to display security warnings to users. 100% of airlines had at least one security finding attributed to expired or invalid certificates which ultimately results in uncertainty for users.

Security Issue – Software Patching

In Software Patching, the top end-of-life software detected by RiskRecon for the airlines were PHP, Nginx, Apache, and WordPress. End-of-life software is no longer supported by the vendor, meaning it won't be patched against new vulnerabilities or security issues that could be discovered. Software like these used by the sample airlines are incredibly common and used by organizations across all sectors, which can make it a large and easy target for cybercriminals to exploit. 85% of the sampled airlines had issues with software patching, among which 313 security findings were identified. While these Software Patching findings are rarer than others provided by RiskRecon, they could present considerable risk to organizations if not mitigated.

Trend – Social Engineering

Beyond the explicit vulnerability findings outlined, cybercriminals often target organizations with poor cybersecurity practices. Criminals may target organizations through social engineering methods such as phishing, which remains an overwhelmingly successful and devastating infiltration method. This is such an issue within the airline industry that Singapore Airlines posted an advisory[17] to customers on September 5, 2023, on phishing scams and good cybersecurity practices. They warn "customers to be cautious of phishing websites, emails, text messages, and phone calls" that claim to be from the airline itself. This is an issue seen across the entire industry seen with reports[18] from July 2023 where the Google listing for multiple airlines like Delta, American, Air France, Turkish Airways, and more displayed fraudulent airline customer service phone numbers. It is vital for organizations and customers alike to remain vigilant on these new tactics utilized by threat actors for deception.

Airports

Airlines work with a myriad of third-party service providers, but the integral role that airports play in enabling modern aviation can't be overlooked.

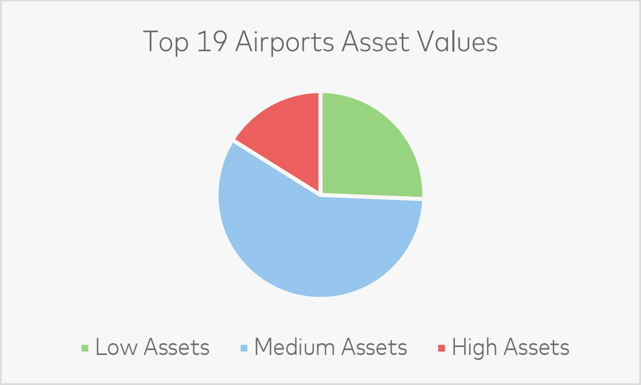
For this reason, this analysis evaluates the cybersecurity posture of the top 19 airports globally based on seats sold in August 2023. Airports have been the target of cyberattacks more recently seen in articles like "German airport websites hit by suspected cyber attack" from February 2023 and "Cyberattacks On U.S. Airport Websites Signal Growing Threat To Critical Infrastructure" from October 2022.

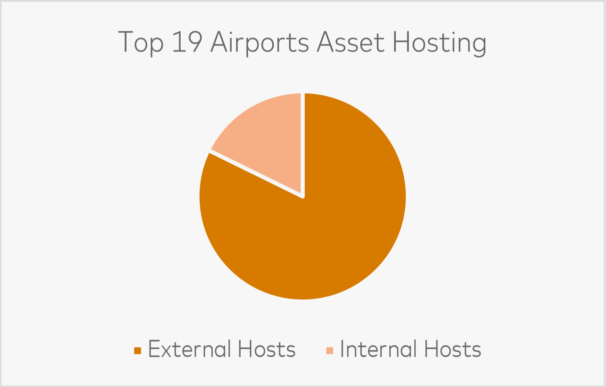
The average overall risk score for the sampled airports is a B (8.2), with 17 of the entities having an A or B score and the remaining two with a score of C or below. Overall, there were 2,161 findings with only five findings with the highest priority which is incredibly promising outlook. Out of those 5 findings, 80% are attributable to airports with a C or below score. On the other hand, there is the concern that 83% of highest priority findings belong to assets that RiskRecon assigned a high

[17] Singapore Air - Advisory on phishing scams and good cybersecurity practices (singaporeair.com)
[18] TheRecord - Called a bogus airline customer support number? Google is hustling to fix that (therecord.media)

value. These are the assets that RiskRecon would prioritize for entities to mitigate first because of the data that is being used within those assets.

The makeup of the top 19 airports is vastly different from the 20 sample airlines. With a median of 43 hosts across an average four hosting countries, the IT profile of the sample airports is much smaller in comparison to the median 510 hosts seen within the sample airlines. They also differ in asset values where airports have 16% of their assets classified at high, opposed to the 2% of high value assets seen with airlines. Where the two align is location where assets are hosted. Though airlines have 96% hosted externally, airports are not far behind with 82%. This could be considered worse due to the larger number of high value assets seen in the airports' IT profiles.





Security Issue – Application Security

Application Security is one of the lowest security domains with an average score of 7.5 and accounts for 57% of the total findings. 98% of the Application Security domain are attributed to missing HTTP Security Headers across 100% of the entities in the sample. This is an issue we see across airlines and airports, exposing that sensitive data open to attackers. Remediating the missing HTTP Security Headers is relatively simple and could alleviate risk for all the airports, removing more than half of the findings within RiskRecon. Along the same lines, the Web Encryption domain had 643 total findings. Out of those findings, 88% of them are due to invalid certificate subjects across 12 of the airports within the sample.

Security Issue – Network Filtering

Within the Network Filtering domain, RiskRecon analyzes the company networks and systems for the presence of unsafe network services and Internet of Things (IoT) devices. These unsafe network services and exposed IoT devices are common vectors used for compromising systems and networks. While there are only 33 findings within the Network Filtering domain, 16 of those findings are tied to Point to Point Tunneling Protocol (PPTP). PPTP is one of the oldest Virtual Private Network (VPN) protocols that are still in use today since being created in the late 1990's. This protocol has many well-known security issues including being vulnerable to basic brute force and decryption attacks.

Conclusion

While the airlines and airports included in our analysis sample performed relatively well, there are still improvements that could be made from all entities. Out of the total 220,644 findings across airlines and airports, the Application Security domain accounts for 51% (112,176) of findings highlighting Application Security as the largest risk area.

The amount of personal information that is handled by the travel industry will continue to be a valuable target for cyber criminals as they select vulnerabilities to exploit in attacks. It is vital that these organizations not only are evaluating own enterprise risk but additionally looking at third-party service providers that enable them to operate daily, especially as the use of third-party service providers continues to expand. In this report, we chose to specifically focus on analyzing airports and their risk, but airlines work with hundreds of third-party service providers. From ground support, warehouses, catering, security, and so many more, each additional third-party service provider adds another layer of risk to consider and handle.

RiskRecon enables monitoring your own organization and the digital ecosystem of third-party (and their vendors') cyber risk based purely on their internet presence. Our unique risk-prioritized action plans rely on advanced models and analytics to prioritize by asset value and issue severity.

Only RiskRecon creates all its own security measurements, comprising more than 40 unique criteria, for the most accurate, deep, and broad picture of risk. RiskRecon finds risks that you may not have known were there. We take it a step further by not just identifying those risks but also by helping your company understand and solve them. RiskRecon helps you manage risk through customized action plans, in-depth security ratings, and actionable insights. Sign up for a demo to see for yourself why RiskRecon by Mastercard is the only solution for managing third-party cyber risk at scale.

Appendix A – Security Domains

Application Security

The Application Security domain assesses each web application for essential, observable application security practices that are leading indicators of the quality of the application security program.

DNS Security

The DNS Security domain assesses the use of controls to prevent unauthorized modification of domain records resulting in domain hijacking. This domain also enumerates the DNS hosting providers to determine level of fragmentation. Control of DNS records is essential to keeping systems accessible. Where domain hijacking controls do not appear to be implemented, the organization should demonstrate compensating controls or implement the recommended domain protection settings.

E-mail Security

The E-mail Security domain assesses the use of authentication and encryption controls necessary to ensure that e-mail messages are not spoofed and that communications are private. The domain also enumerates the e-mail hosting providers, providing visibility into the e-mail hosting providers. Organizations should consistently implement e-mail encryption for all servers and e-mail authentication for all domains. Where the organization has a high number of e-mail hosting providers, the organization should be asked to explain how they defend e-mail bourn threats emanating through each provider system.

Network Filtering

The Network Filtering domain enumerates unsafe network services and Internet of Things (IoT) devices the organization has exposed to the internet. Enterprises should limit Internet-accessible network services and systems to those that are safe and necessary. Unsafe network services and IoT devices are very susceptible to compromise through various methods such as credential guessing, communications intercept, and vulnerability exploitation. RiskRecon analyzes Internet-facing systems and networks for the following services: MS SQL Server, MySQL, PostgreSQL, MongoDB, Elastic, DB2, Redis, Memcached, CouchDB, Cassandara, Remote Desktop Protocol, VNC, Telnet, FTP, Samba, Finger, NetBIOS, BGP, PPTP, X11, Oracle TNS, Apple Airport, Webmin. RiskRecon analyzes systems and networks to discover Internet of Things (IoT) devices, such as printers, elevator control systems, HVAC interfaces, cameras, and network storage devices.

Software Patching

The Software Patching domain enumerates systems that are running end of life and vulnerable software. Because end of life software is not supported by the vendor, it cannot be patched against known security issues or new vulnerabilities that might be discovered. All software patching issues should be addressed immediately, and software patching practices should be modified to ensure that software remains current going forward. Further details are provided in the downloadable Software data file.

System Hosting

The System Hosting domain analyzes the hosting practices of the organization, enumerating the hosting providers and the countries that systems are hosted in. It is essential to ensure that systems are hosted in reputable countries and that the host country data privacy laws are obeyed. High fragmentation of hosting with a large number of hosting providers is a leading indicator of gaps in I.T. governance.

System Reputation

RiskRecon analyzed I.P. reputation and threat intelligence databases to identify suspicious system activity. Observed malicious activity may indicate the system is compromised or is being used for unauthorized purposes. Of the issues identified, Mastercard - Sandbox selected those detailed in this section as important to investigate and address due to the issue severity and the sensitivity of the system in which the issue exists.

Web Encryption

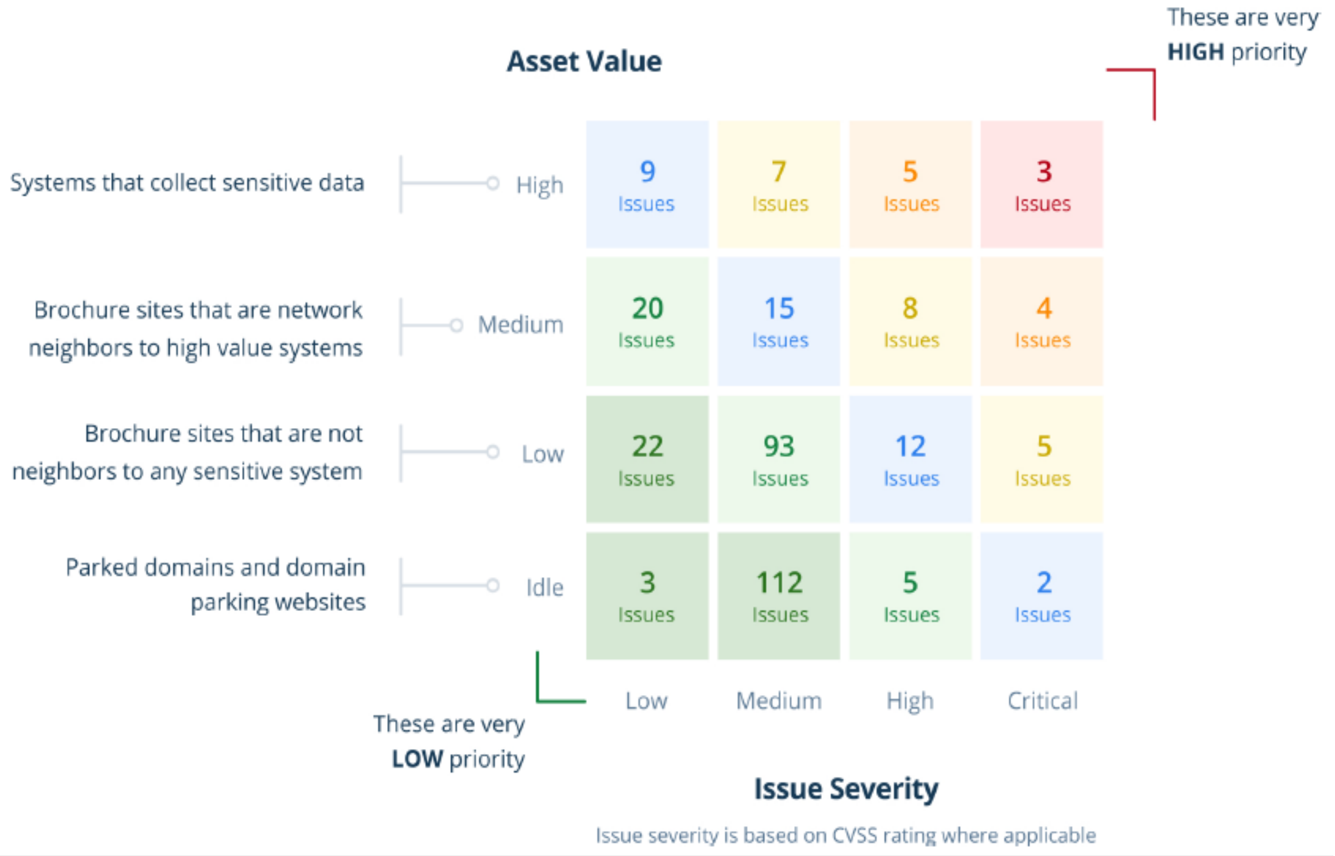
The Web Encryption domain analyzes the effectiveness of encryption implementations, determining if they are properly configured to prevent errors, use secure protocols and apply minimum key lengths necessary to ensure communication privacy. All encryption errors should be addressed to prevent encryption errors being displayed to users and to ensure that the encryption implementation is effective.

Breach Events

The Breach Event domain summarizes the breach events the organization has experienced. Recent breach events indicate gaps in the breach protection program. Organizations with breach events occurring consistently over time likely have ineffective breach prevention programs and material gaps in their information security program. Organizations with recent and repeated breach events over time should be examined closely to ensure that controls are operating effectively to prevent future breaches and loss of data.

Appendix B – Security Issue Findings

RiskRecon risk prioritizes every issue based on the severity of the issue and the value of the asset in which the issue exists. RiskRecon uses the Issue Priority Matrix to visualize risk. Issues become increasingly severe from left to right of the matrix, and assets become more and more value from bottom to top. Issues in the top right quadrant are the most severe ones found on higher-value assets, which need immediate attention and a quick fix. On the contrary, issues in the bottom left quadrant are the less severe ones found on lower-value assets, which should be evaluated but may not require an immediate fix.



These are very **HIGH** priority

Asset Value

		Low	Medium	High	Critical
Systems that collect sensitive data	High	9 Issues	7 Issues	5 Issues	3 Issues
Brochure sites that are network neighbors to high value systems	Medium	20 Issues	15 Issues	8 Issues	4 Issues
Brochure sites that are not neighbors to any sensitive system	Low	22 Issues	93 Issues	12 Issues	5 Issues
Parked domains and domain parking websites	Idle	3 Issues	112 Issues	5 Issues	2 Issues

These are very **LOW** priority

Issue Severity

Issue severity is based on CVSS rating where applicable