REPORT

The Cyber Risk Landscape of the Global Aviation Industry

SecurityScorecard

Introduction

In June 2024, SecurityScorecard researchers analyzed cyber risk across the aviation industry. We examined airlines and the various types of vendors they rely on – such as manufacturers, ground handling service providers, and industry-specific information technology (IT) providers.

Historically, the aviation industry's extensive security and safety programs have concentrated on physical risks, such as mechanical flaws and terrorist threats. To bolster cybersecurity across the aviation industry, this research aims to elevate the priority of cyber risk within the industry's critical security and safety discourse. Recent revelations from within Boeing have heightened concerns about physical safety risks from within the industry's extensive supply chain. This research aims to raise similar awareness of cyber risks within the industry's supply chain as well.

> *"Third-party cyber risk impacts all industries, but some industries are more vulnerable and severely affected due to the nature of their business and larger third-party networks."*

Regulatory responses to cybersecurity concerns

New regulations aim to bolster aviation cybersecurity in response to such concerns. In the U.S., the Transportation Security Administration introduced new cybersecurity requirements for airports and airlines in March 2023. Similarly, in the E.U., Implementing Regulation 2023/203, a framework for information security risk management in aviation, takes effect in 2026.

As the aviation industry grapples with supply chain cyber threats, understanding these risks' entire scope and impact is crucial for developing effective mitigation strategies. The following key findings from our research provide a detailed look at the vulnerabilities within the aviation supply chain and highlight areas where heightened security measures are essential. These insights aim to guide cybersecurity leaders in fortifying their cybersecurity posture, ensuring safer and more resilient aviation operations in an increasingly interconnected digital landscape.

Key Findings

The aviation industry gets a “B” grade for cybersecurity

Airlines have higher average security ratings than: the aviation industry in general, by one point; manufacturers of aircraft and components, also by one point; aviation services vendors, by two points; and aviation-specific technology vendors, by three points. Accordingly, these vendors pose more third-party cyber risks to their airline customers.

Lowest scores for Software & IT Vendors

Aviation-specific software & IT vendors have the lowest scores in the industry, with a mean of 83 and a median of 86, posing even more third-party risks for their airline customers. Software and other IT products and services in general enable as much as 75% of third-party breaches across all industries.

Impact of Third-Party Breaches

Airlines had 4% more breaches and compromises than the industry-wide norm, despite their higher security scores. We attribute this discrepancy to the third-party risks they incur from their lower-scoring vendors.

Customers contribute to third-party risk

In addition to the usual focus on vendors, we found three examples of airline compromises that exposed data on their vendors.

Advanced economies achieve better cybersecurity outcomes

Average aviation industry security scores trend higher in advanced, affluent economies than in emerging markets, with the one higher-performing exception of Latin America.

Performance correlation

Airlines with the best performance rankings from aviation & travel industry analysts and consumer publications have above-average security ratings. Average scores for budget airlines are nearly the same as those of full-service airlines.

AppSec is the top weakness in attack surfaces

Application Security is the most common area (34% to 48%) in which aviation organizations score lowest. The most common Application Security issues that have the worst impact on scores are HTTP usage in redirect chains and the lack of two key attributes in session cookies.

Breach and incident tracking

7% of our sample had publicly reported breaches in the past year, 17% had at least one compromised device on their networks in the past year, and 3% had both. 21% thus had either confirmed breaches or potential compromises.

Ransomware is the top cyber threat

Based on public reporting, ransomware is the top cyber threat to the industry. Other incidents highlight the theft of passenger data, either by criminals for financially-driven fraud, or by governments for intelligence purposes.

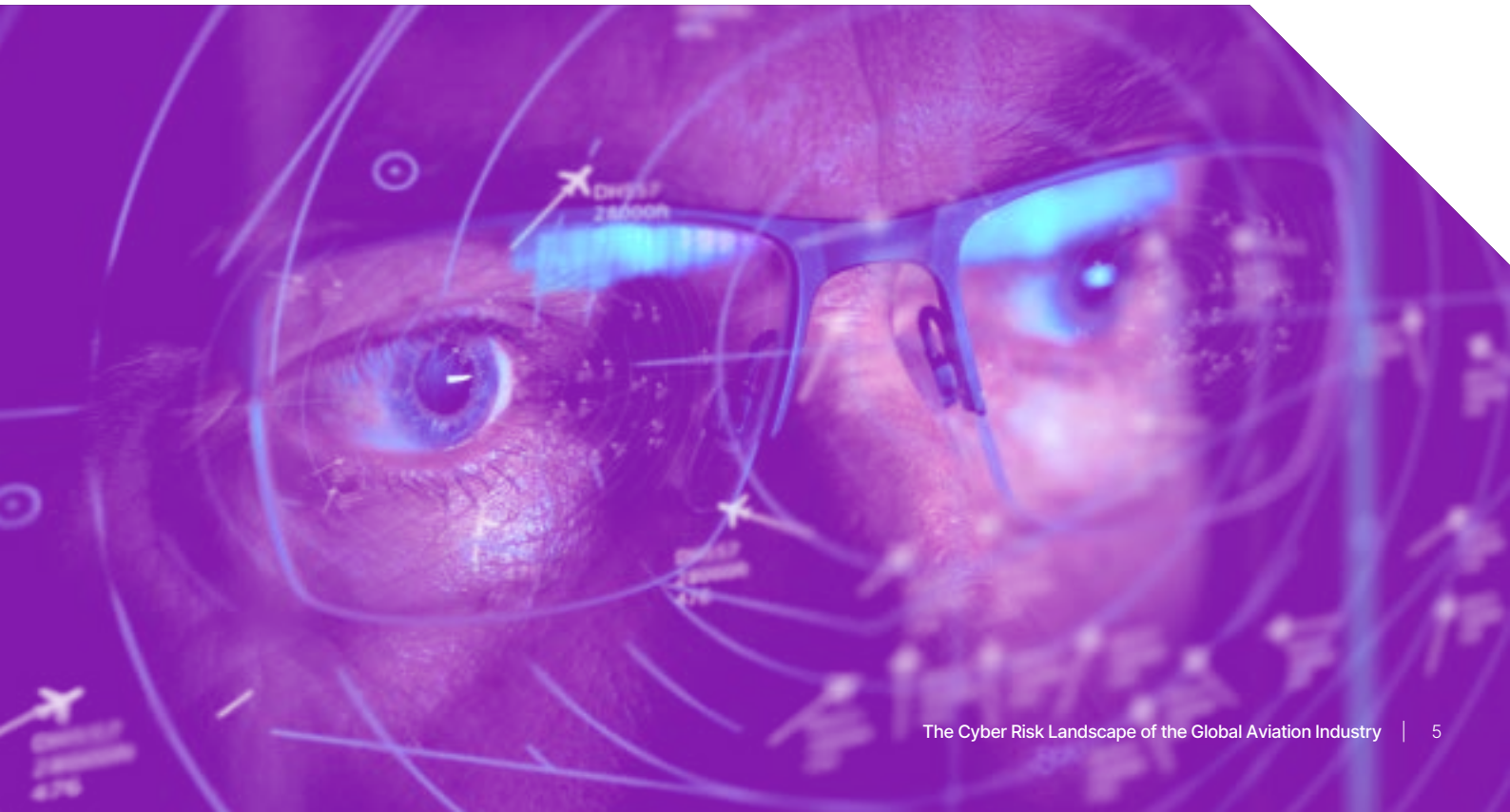
Methodology

SecurityScorecard compiled a sample of 250 organizations, including:

- 100 top-rated commercial passenger airlines
- 50 top manufacturers of aircraft and their components
- 50 top providers of aviation services, such as ground handling and maintenance, repair & overhaul (MRO)
- 50 top providers of aviation-specific software & IT products and services

We built this list from industry rankings and trade and consumer publications, based on a mix of financial, quantitative, and performance metrics and strategic significance. For each company, we noted:

- Security score, based on our collection and analysis of signals from its attack surface
- Lowest-scoring security factor and its score in that area
- Issue with the most negative impact on its score
- Any publicly reported breaches in the past year
- Any evidence of compromised machines in the past year



General Statistics

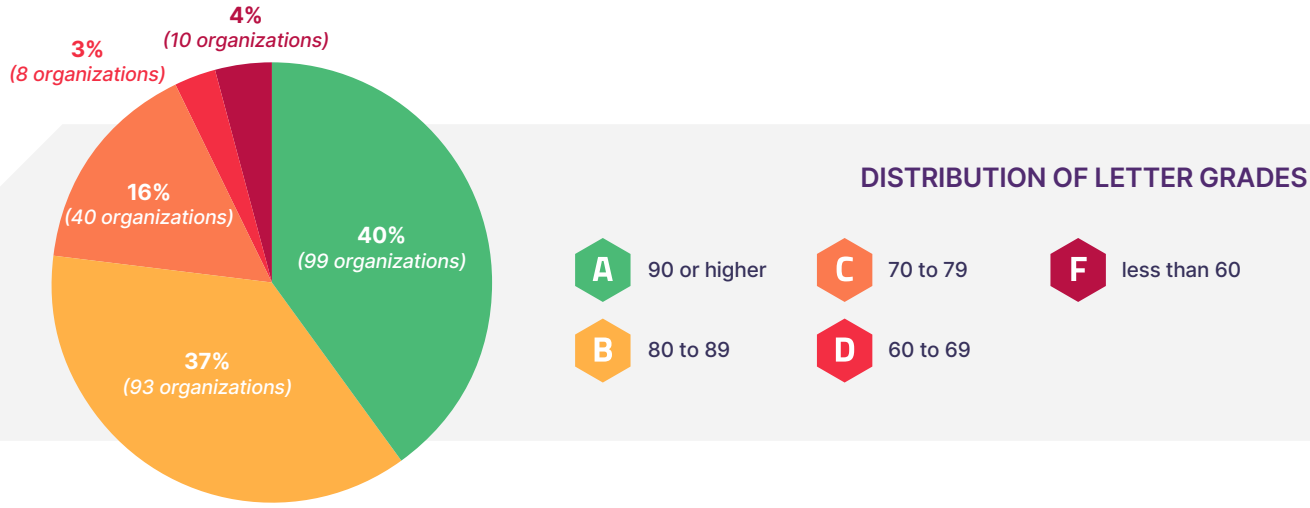
The mean score for the whole aviation sample was 85; the median score was 88. The gap between the mean and the higher median indicates that the sample is somewhat "left-skewed." In other words, a few extremely low scores are dragging down the mean value.

For comparison, the global mean score for the more than 12 million organizations in our platform worldwide and across all industries is 86.

Distribution of Letter Grades

77% of our sample had either strong "A" or good "B" security ratings.

According to our ratings methodology, a "B" rating indicates a 2.9x greater likelihood of a breach than an "A"; a "C" rating indicates a 5.4x greater likelihood of a breach; a "D" rating indicates a 9.2x greater likelihood of a breach; and a "F" rating indicates a 13.8x greater likelihood of a breach.



Sector-Specific Scores

Airlines have the highest mean and median scores, outperforming the whole sample by 1 point. The other three sectors, whose mean and median scores match or are lower than the overall sample, are vendors for airlines. These uneven scores mean that higher-scoring airlines are on the receiving end of greater third-party risk from their lower-scoring vendors, who are at greater risk of compromise and passing on those risks to their airline customers. In other words, the greater security risks of airlines' vendors weaken the otherwise more robust security of those airlines.

> *"A company's security is only as strong as its weakest link."*

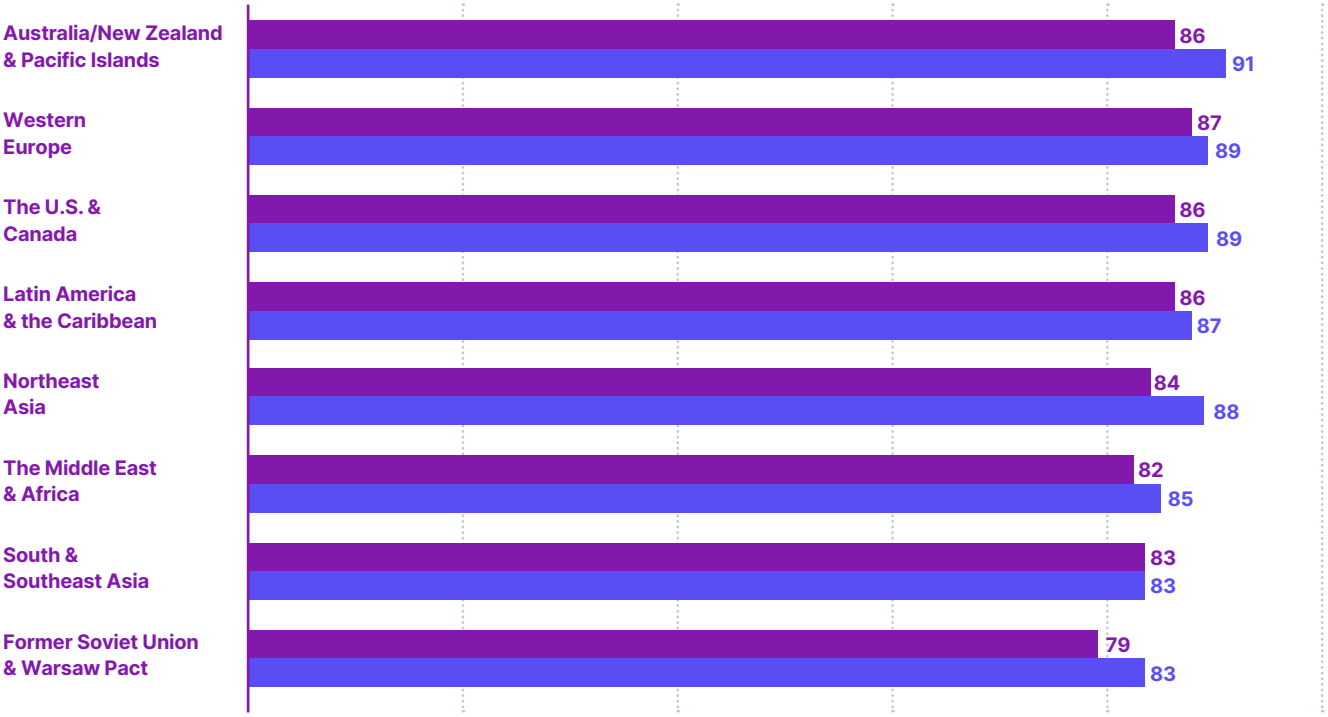
The lowest mean and median scores are for aviation-specific software & IT vendors. As previous SecurityScorecard research showed, software & IT vendors in general tend to be higher-risk, receiving lower scores in our platform. Among other findings, our prior research found that software & IT vendors have third-party breaches at rates higher than in other industries and that vendors' software & IT products and services enable three-quarters of third-party breaches.

This higher level of third-party risk compounds when it is heavily concentrated in a relatively small number of vendors with enormous market share. If nothing else, software & IT vendors are more vulnerable simply due to their typically larger, more complex, and more "cyber-intensive" attack surfaces compared to more "brick and mortar" businesses focused on the physical realm. They pass this heightened risk on to their customers – in this case, airlines.

Regional Security Scores

The aviation industry has a heavily international orientation. Aside from the global travel that many airlines enable, its supply chains and other relationships frequently cross borders. To what degree, if any, do security ratings vary by geography?

MEAN AND MEDIAN SECURITY RATINGS BY GEOGRAPHIC REGION

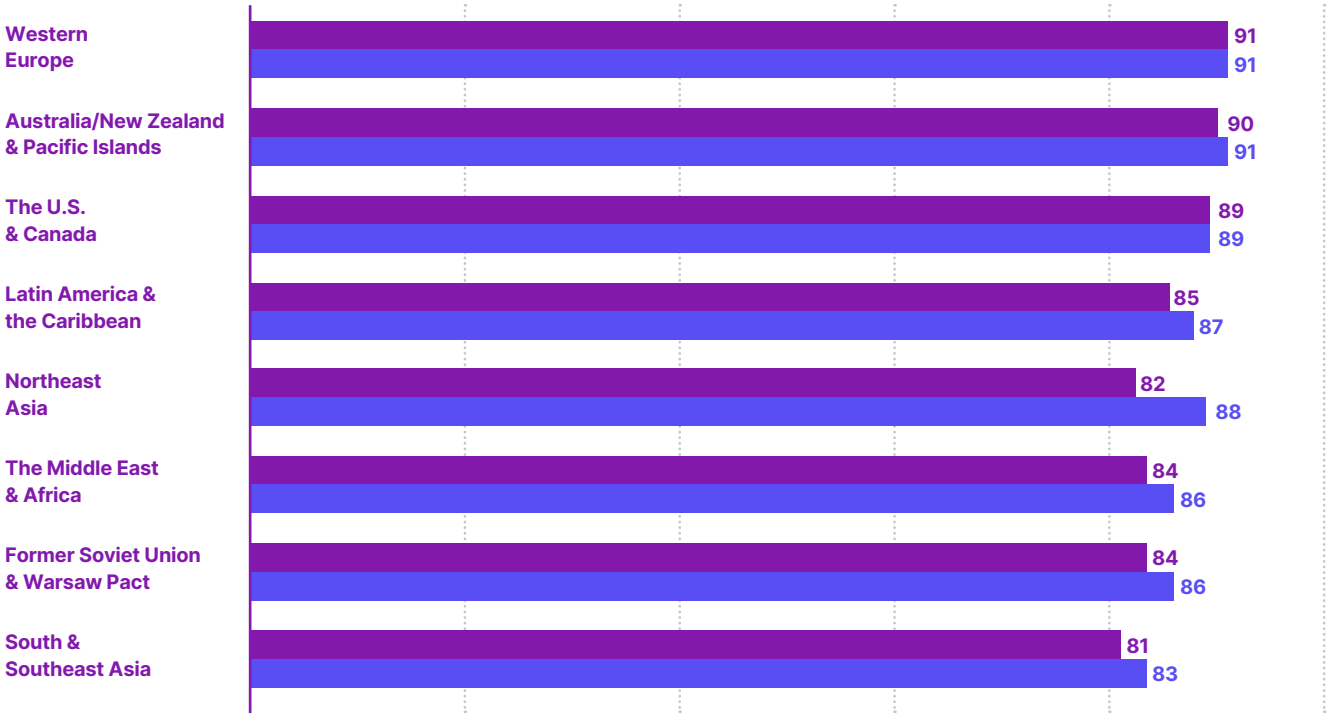


Prior SecurityScorecard research established a correlation between security hygiene and economic development. Organizations in advanced, affluent economies typically have more robust security than those in developing or otherwise challenged economies. Security costs money: those with more funding are more likely to afford security investments. These results are consistent with this finding, except that Latin America & the Caribbean ranked higher than expected. We attribute these unexpectedly high ratings to organizations in our sample from Brazil, which has a larger and more developed economy than many of its neighbors.

Variations Amongst Airlines

We further inquired whether this geographic pattern holds true for airlines in particular. The pattern is similar, albeit with one unusually low score dragging down the mean for Northeast Asian airlines. In such a markedly "left-skewed" data set, in which the median (88) is much higher than the mean (82), the former value is probably a more accurate reflection of the whole set of values.

MEAN AND MEDIAN SCORES FOR AIRLINES BY GEOGRAPHIC REGION

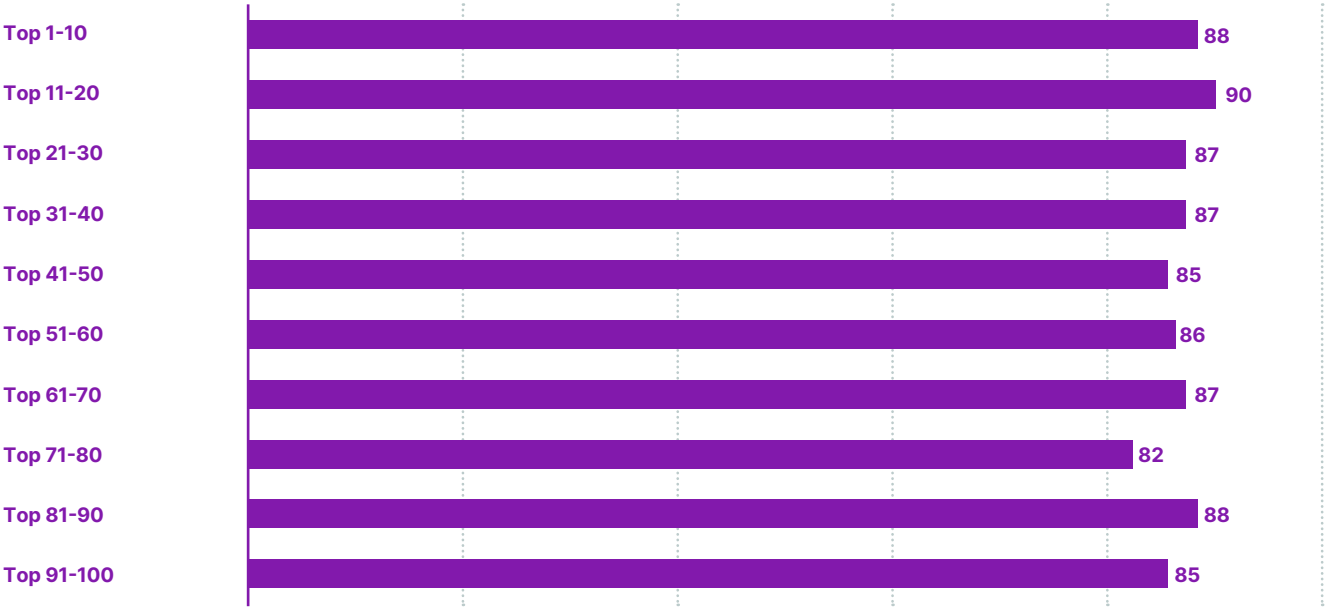


Cybersecurity ratings are one way of evaluating airlines. The aviation and travel industries, trade publications, and consumer-oriented travel publications also evaluate and rank airlines. Standards and performance ratings for these evaluations include factors such as safety records, on-time arrivals, delay rates, customer complaint rates, lost luggage rates, and so on. We thus asked: Do more highly-rated airlines in general have higher security scores as well?

Variations Amongst Airlines *(continued)*

We found a partial correlation. The top 20% of airlines, ranked by industry performance standards and according to travel and consumer analysts, had above-average security scores (88-90). The next 20% also had slightly above-average scores (87). Below that top 40%, scores are average or below-average, but the downward trend is inconsistent and even reverses itself at first. That top 20% of our airline sample includes those airlines often described in industry/travel publications as high-end/premium airlines or top performers, such as Singapore Airlines, Cathay Pacific, Japan Airlines, Qatar Airways, Emirates, Al Etihad, Turkish Airlines, and Air France.

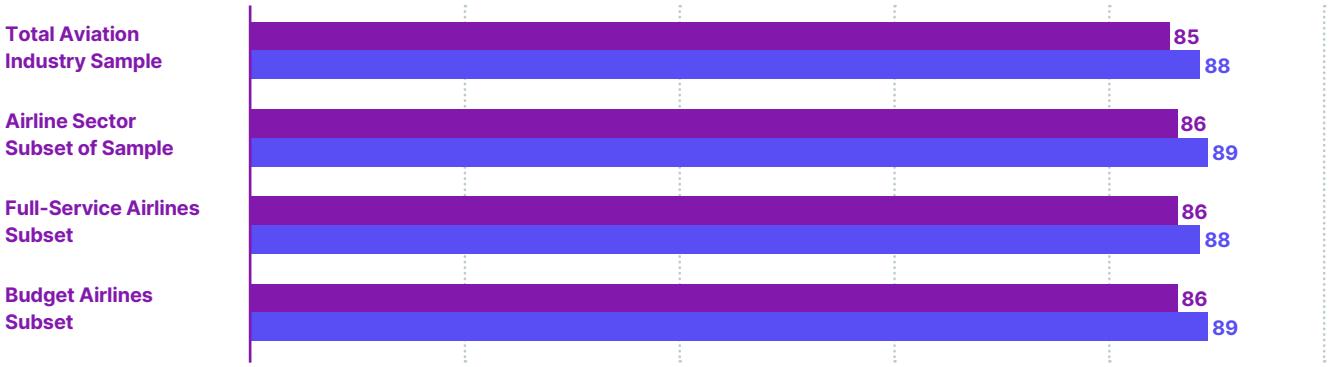
AVERAGE SECURITY SCORES FOR EACH 10% OF AIRLINE INDUSTRY RANKINGS



By the same token, is there any difference in security scores between full-service carriers (FSCs) on one hand and budget airlines or low-cost carriers (LCCs) on the other? The latter offer lower base fares by charging for extras or by cutting corners to create savings to pass on to consumers. Cybersecurity is a major investment, and it stands to reason that some cost-saving measures might weaken it. In this case, however, the LCC business model had no appreciable impact on security ratings. 33 of the 100 airlines in our sample are LCCs. Their mean security score was 86, and the median was 89 - the same values as the total sample of 100 airlines, including 67 FSCs. In fact, those 67 FSCs had a slightly lower median score of 88 but the same mean score.

Variations Amongst Airlines *(continued)*

MEAN AND MEDIAN SECURITY RATINGS FOR FULL-SERVICE AND LOW-COST AIRLINES



The combination of the two findings above may seem counterintuitive. Top-performing airlines have above-average security scores to parallel their higher rankings and performance metrics, but the security scores of FSCs and LCC are largely the same. Funding is a significant variable in security ratings, but it does not tell the whole story. The partial correlation between our security ratings and airline ratings may suggest that some organizations are simply better at what they do, cyber or otherwise.

Sufficient funding is key to achieving a degree of cyber health, but merely throwing more money at problems does not solve them either. One can reach a point of diminishing returns at which more investments become less effective; at some point, skill and vigilance can become more important factors. In other words, the LCC model has not prevented budget airlines from spending enough to achieve good cyber security. Still, the higher performance standards of top-rated airlines have extended to their cyber security as well.

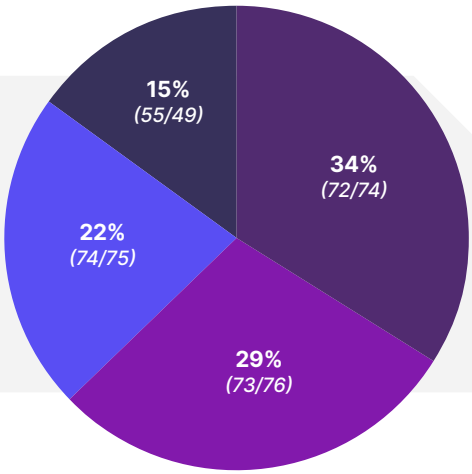
Problem Areas

General Security Factors

For each organization in our sample, we identified one of 10 security evaluation factors for which it received the lowest score and the values of those lowest scores.

PERCENTAGES OF ORGANIZATIONS WITH THEIR LOWEST SCORES IN EACH SECURITY FACTOR, WITH MEAN & MEDIAN SCORES OF THOSE ORGANIZATIONS FOR THOSE SECURITY FACTORS

- **Application Security:** 34% (72/74)
- **Network Security:** 29% (73/76)
- **DNS Health:** 22% (74/75)
- **Endpoint Security:** 15% (55/49)

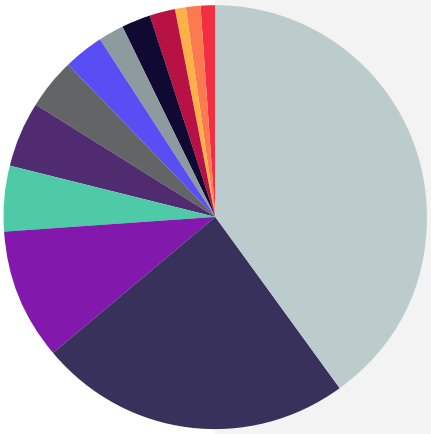


Endpoint Security is the outlier in this data set. It is the least common of the four main security factors among the lowest scores in our sample. At the same time, mean and median Endpoint Security scores for organizations with their lowest scores in this risk factor are significantly lower than those for the other three main risk factors. In other words, Endpoint Security is the least common area for organizations to have their lowest scores. Still, it has a far more substantially negative impact on their scores in those less common cases. In comparison, the other risk factors are more common as the sources of lowest scores, but they tend to have a less severe impact on organizations' overall scores in those more common cases.

Problem Areas *(continued)*

Specific Security Issues

We looked further into our data set to identify the specific issues that had the most negative impact on organizations' overall scores. This approach further emphasized the dominance of Application Security issues as the most common sources of the greatest score-lowering risk, as the figures above indicated, but even more so. Application Security issues accounted for 48% of the issues with the most negative score impact. The single most common issue, however, was the use of weak SSL/TLS protocols, a Network Security issue common across all industries.



SECURITY ISSUES WITH MOST NEGATIVE SCORE IMPACTS

- **SSL/TLS Service Supports Weak Protocol (Network Security):** 40%
- **Redirect Chain Contains HTTP (Application Security):** 24%
- **Session Cookie Missing "Secure" Attribute (Application Security):** 10%
- **Session Cookie Missing "HTTPOnly" Attribute (Application Security):** 5%
- **Outdated Web Browser Observed (Endpoint Security):** 5%
- **Website References Object Storage (Application Security):** 4%
- **SPF Record Contains a Softfail without DMARC (DNS Health):** 3%
- **SPF Record Missing (DNS Health):** 2%
- **Unsafe Implementation of Subresource Integrity (Application Security):** 2%
- **Website Copyright is Not Current (Application Security):** 2%
- **Certificate without Revocation Control (Network Security):** 1%
- **DNS Server Accessible (Network Security):** 1%
- **Miscellaneous Application Security Issues:** 1%

The single-most common Application Security issue was the use of HTTP in redirect chains. This practice risks exposing data to interception and manipulation, including man-in-the-middle (MITM) attacks and rerouting users to attack infrastructure for phishing or other purposes.

The next two most common Application Security issues involve attributes missing from session cookies. The lack of "secure" attributes enables cookie transmission via HTTP connections, running the risk of interception by attackers, who can use them to gain access. The lack of "HTTPOnly" attributes allows client-side scripts like JavaScript to access them, increasing the risk of cross-site scripting and other attacks with which attackers can hijack sessions.

Outdated web browsers are the only Endpoint Security issue that surfaced in any significant numbers in our data set. These outdated web browsers must be the source of the highly negative score impact on the relatively small number of organizations that scored lowest in this area. Outdated browsers expose endpoints to the exploitation of vulnerabilities that remain unpatched.

Two other issues stood out as DNS Health risks. Sender Policy Framework (SPF) records greatly reduce spoofing of an organization's email addresses by listing authorized senders for its domain, which recipients use to verify that a message from that domain came from a legitimate sender.

Domains without SPFs are easier targets for email address spoofing, facilitating phishing attacks. On the recipient side, Domain-based Message Authentication, Reporting, and Conformance (DMARC) should reject email messages that fail SPF checks. At some organizations, however, they merely "soft fail" and still reach spam folders or even inboxes, albeit with suspicious markings. Such a "soft fail" leaves users at greater risk of exposure to malicious email messages.

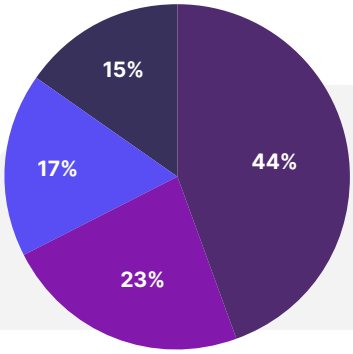
Confirmed and Potential Breaches and Compromises

One goal of these ratings is to gauge an organization's risk of a breach. Our platform collects open-source reporting on breaches from various sources, including news reports, security research, and press releases. A review of this coverage indicated that 17 of the 250 organizations in our sample, or almost 7%, experienced publicly reported breaches within the past year.

Such reporting cannot claim to be comprehensive. It requires both the detection of the breach and its disclosure to the public by victims, attackers, journalists, or security researchers. Breaches often go undetected by victims and researchers for extended periods, and there may be further delays before a detected breach becomes public knowledge (if ever).

We thus supplemented this publicly reported breach coverage with select findings from the IP Reputation score factor that indicate possible malware infections or other compromises at an organization. These findings do not necessarily indicate a full-scale breach or compromise of the organization in question. Indeed, they could mean little more than precisely what they indicate: the infection or compromise of at least one machine in the past year. They can nonetheless shed light on potential breaches that the press has not reported yet or that victims may not have detected yet. A compromised machine could be just the tip of the iceberg, or an initial access point from which a threat group moves laterally and expands its access across the network.

This query indicated that 43 organizations, or 17% of our total sample, had evidence of at least one compromised machine on their networks in the past year. This set of 43 organizations had some overlap with the set of 17 organizations with publicly reported breaches. 8 organizations, or 3% of our sample, had both publicly reported breaches and evidence of at least one compromised machine on their networks. It is unclear if the evidence of compromise our platform detected was related to the reported breaches at these organizations. We merged the list of 17 organizations with reported breaches and the list of 43 organizations with at least one potentially compromised machine and removed the 8 duplicates. This process yielded a final list of 52 confirmed or potentially compromised organizations, representing 21% of our sample.



DISTRIBUTION OF CONFIRMED BREACHES AND POTENTIAL COMPROMISES BY SECTOR

- **Commercial Passenger Airlines:** 44%
- **Manufacturers of Aircraft & Their Components:** 23%
- **Aviation Services, Ground Handling, and MRO:** 17%
- **Aviation-Specific Software & IT:** 15%

This distribution of confirmed and potential compromises by sector seems counterintuitive at first. Airlines represented 40% of our total sample but a somewhat higher (44%) proportion of this subset of our sample with confirmed breaches and potential compromises. The higher scores of airlines, compared to their vendors in the other three sectors, suggest that they should experience fewer breaches or compromises rather than more of them, as in this case.

Case Studies of Publicly Reported Breaches

Third-Party Breaches

A review of public reporting on the breaches in this sample suggests that third-party risk explains some of this discrepancy. As mentioned earlier, the airlines may have the highest scores but incur more third-party risk from their lower-scoring vendors in the other three sectors.

For example, a publicly reported breach in our sample was a third-party breach involving an IT vendor that exposed information on 8,800 pilot applicants at two U.S. airlines. The two airlines were in our sample, but the IT vendor would have had to be more significant in the industry to warrant inclusion in our sample. This breach thus counted toward the airline's sector breach total because it affected two airlines, but it ultimately originated with the IT vendor. The two U.S. airlines had used this vendor to manage online hiring processes for pilots. In the wake of this incident, they decided to use internal IT resources to manage future pilot applications instead.

Other aviation-specific software & IT vendors with a larger footprint have become victims, too. For example, in September 2023, the Dunghill Leak ransomware group claimed to have compromised U.S-based travel reservation software developer Sabre and compromised 1.3 TB of data, publishing a sample of it. The purportedly compromised data included airline ticket sales and passenger data, personal data on Sabre employees, and Sabre's corporate financial records. Sabre provides software for airlines, hotels, and other travel-related businesses. It was unclear what, if any, third-party repercussions this breach might have had for airlines using Sabre's booking software beyond the exposure of select ticket and passenger data.

The technology for physical security systems is another sensitive target for this industry, given the extensive physical security restrictions around airlines' ground operations and the sensitivity of aviation hardware. For example, French aerospace manufacturer and aviation services provider Thales, along with several other organizations, experienced a third-party data breach in June 2023 via its physical access control systems vendor, Belgium-based Automatic Systems. The BlackCat ransomware group claimed responsibility for this attack and released data samples from Automatic Systems' customers, including Thales. BlackCat claimed that Automatic Systems' customers were at risk of physical security breaches due to security vulnerabilities in its access control products that BlackCat claimed to have identified. If there was any truth to that claim, such product security vulnerabilities could at least theoretically enable physical access compromises

Case Studies of Publicly Reported Breaches
(continued)

at customer locations, thus exposing Thales' portion of the aviation supply chain. Thales' aviation business areas include aircraft avionics components, in-flight entertainment systems, air traffic control systems, and MRO services.

Of course, airlines and companies in other sectors of the aerospace & aviation industry have vendors outside the industry that have little or nothing to do with aviation. While software & IT vendors are top sources of third-party risk in this regard, other vendors of non-technical products and services can enable third-party breaches as well – up to 25% of them, according to previous SecurityScorecard research. Typical sources of third-party breaches from non-technical vendors include law firms, consultants, accountants, and other professional services firms. For example, a BlackCat ransomware attack on Australian law firm HWL Ebsworth exposed confidential information on its clients, including Rex Airlines, a regional airline in Australia.

Another incident that affected two airlines in 2023 - British Airways and Irish flag carrier Aer Lingus - provides another example of third-party risk from non-aviation vendors and an example of fourth-party risk - in this case, via vulnerable software used by a non-technical vendor. The UK-based HR and payroll service Zellis was one of many victims of a massive global campaign by the criminal group "C10p" to exploit a zero-day vulnerability (CVE-2023-34362) in Progress Software's MOVEit file transfer software in mid-2023. The compromise of Zellis exposed personal information on current and former employees of companies that used its HR and payroll services, including those two airlines.

Case Studies of Publicly Reported Breaches
(continued)

Customers Are Another Source of Third-Party Risk

Business-to-business (B2B) relationships are a two-way street, including cyber risks. The tendency is to focus on vendors as a source of third-party risk for their customers, but it can also work the other way around. Compromised customers can expose information on their vendors as well. For example, a September 2023 BianLian ransomware attack on Air Canada purportedly exposed information on that airline's vendors and suppliers. However, the airline's characterization of the extent of the breach and the affected data was more limited. The group claimed to have compromised 210 GB of Air Canada data. Beyond vendors and suppliers, the compromised data reportedly included employee information (which the airline acknowledged) and technical, security, and other operational details of the airline dating back as far as 2008.

Another ransomware attack on an airline also illustrated that compromised customers can expose information on their vendors. In March 2024, the "SiegedSecurity" threat group claimed to have compromised AirAsia, Malaysia's largest airline and Asia's largest budget airline. The group released a sample of 2.2 GB of purportedly compromised AirAsia files. Those files included detailed information on its vendors, such as email addresses and bank accounts.

Another August 2023 breach reinforced this point that vendors face third-party risks from their customers. Indeed, this breach illustrated it twice, creating a fourth-party and third-party breach. An employee unwittingly enabled unauthorized access to the infrastructure of one of his employer's vendors, which compromised employee information for that vendor's vendors. The attacker posted information on 3,200 employees of vendors of Airbus, one of the two main manufacturers of commercial passenger aircraft. The vendors included companies such as the Thales company mentioned above, which provides components for the aircraft that Airbus manufactures. The attacker obtained this information by compromising credentials for an Airbus customer portal belonging to an employee of Turkish Airlines, an Airbus customer.

Case Studies of Publicly Reported Breaches
(continued)

Various Types of Attacks

Ransomware and other extortion are top threats to organizations across all industries, including this one, as the above examples indicate. The amount of ransom demands has been trending upwards in general. However, specific demands often reflect a company's measurable financial value based on metrics such as its annual revenue or market capitalization. Larger companies are thus more likely to receive higher ransom demands. Accordingly, Boeing, one of the two dominant manufacturers of commercial passenger aircraft worldwide, received one of the two largest-ever reported ransom demands: $200 million USD. The ransomware group LockBit claimed to have compromised Boeing in October 2023 and released 43 GB of purportedly compromised data after Boeing refused to pay this enormous ransom.

Criminals are not the only threat actors targeting this industry. State-sponsored threat actors also target aerospace & aviation organizations for various reasons, ranging from the theft of high-value aerospace intellectual property to the collection of passenger data in support of intelligence operations. The latter use case applies to the state-sponsored Chinese cyber espionage compromise of Air Astana, the flag carrier airline of Kazakhstan. This breach came to light via a leak of files from iSoon/Anxun, a Chinese Ministry of Public Security vendor with a possible nexus to APT41. The main targets of this cyber espionage campaign were not airlines but Kazakhstan's telecommunications service providers, suggesting that its goal was to collect information on the movements and other activities of Kazakh citizens.

Passenger data has value for criminals as a source of personal details for identity theft, such as dates of birth and passport numbers. This use case may have motivated a November 2023 breach of Gulf Air, the flag carrier of Bahrain. While the exact circumstances of the attack remain unclear from public reporting, the other available details were not indicative of a ransomware attack. Instead, the purported attacker offered to sell purportedly compromised Gulf Air passenger records just a few days later. Ransomware attackers often sell compromised data from victims who refuse to pay ransom, but the time between this breach and this offer would have been relatively short for a failed ransomware negotiation (if there was any). His price of $70,000 was for 200 million passenger records dating from the airline's establishment to the present.

Conclusions and Recommendations

Prioritize Software & IT Vendors for Third-Party Risk Management

Software & IT vendors, including those with products and services specific to aviation, should be a top priority for airlines' third-party risk management (TPRM) programs. The lower average scores of aviation-specific software & IT vendors put their higher-scoring airline customers at greater risk. More generally, software & IT vendors in general, across all industries, are top enablers of third-party breaches and tend to have more exposed and vulnerable attack surfaces.

Third-Party Risk Management Should Cover Vendors, Customers, and other Partners

There is a tendency to use the terms TPRM and vendor risk management interchangeably as if they were the same thing - but they are not. Vendors may be top sources of third-party risk, but they are not the only ones. Compromised customers can expose information on, or the infrastructure of, their vendors, too, as we saw in three cases from this sample. Add customers to your TPRM coverage if they have access to your sensitive data or infrastructure. Ensure that your TPRM programs cover other partners that are neither customers nor vendors. In this industry, examples of such relationships could include:

- Fellow airline alliance members or other airlines with which you have flight code sharing or joint ticketing arrangements
- Other travel businesses with whom you have partnerships, such as online travel agencies, hotel chains, and car rental agencies
- External loyalty programs
- Financial institutions issuing co-branded airline credit cards

Session Cookies and SPF Records

Two common security issues in this industry sample warrant special consideration relative to the typical attack surfaces of airlines. The lack of "Secure" and "HTTPOnly" attributes in so many website session cookies could jeopardize customer credentials, potentially enabling fraudulent purchases, identity theft, and other malicious activities. Ensure that your customer-facing websites have these attributes in their session cookies. Organizations lacking SPF records are at greater risk of malicious spoofs of their email addresses. Threat actors could facilitate attacks on airline customers by spoofing messages that customers routinely receive from airlines, such as reservations, flight status updates, marketing campaigns, or periodic updates on their loyalty program accounts. Ensure that your domains have SPF records, and do not let messages that "soft-fail" your SPF checks reach your users' inboxes or spam folders.

Conclusions and Recommendations *(continued)*

Protect Intellectual Property and Passenger Data

Security programs should clarify which of their data sets and other assets threat actors are most likely to target. The goal is to improve defenses around those key assets and increase the odds of detecting attempts to compromise them. Aerospace intellectual property is of high value to state-sponsored threat actors and criminals and thus deserves special consideration for those organizations with access to it. The reporting on incidents from our sample also highlights the value of passenger data for both criminals and state-sponsored actors, so it also deserves special attention. Criminals may seek it for its value as an ingredient in identity theft or as a digital hostage for the extortionate demands of a ransomware attack. Foreign intelligence services also value airline passenger data as a way to identify and track persons of interest.

Avoid Paying Ransoms

SecurityScorecard does not recommend paying ransoms, but we also recognize that, in some situations, victims may have few or no alternatives. Organizations considering ransom negotiations and payments must nonetheless recognize that it is not a silver bullet; it comes with its own risks. Organizations considering this path should seek legal advice, as some jurisdictions have begun banning ransom payments. Sending funds to ransomware operators in jurisdictions like North Korea, Iran, or Russia could also run afoul of U.S. or international sanctions.

Aside from purely technical errors that may prevent sincere ransomware operators from restoring encrypted files as promised, unscrupulous ransomware operators pose multiple risks for victims who pay ransoms. The most obvious risk is that they simply will not keep their word. Compliance with the file decryption terms of a ransom deal is easy enough to verify, but ensuring the confidentiality of compromised files is not. Attackers can easily sell compromised files to other criminals without the knowledge of victims who paid to maintain the confidentiality of those files, leaving attackers with less incentive to keep their word. More insidious is the perception of willingness to pay ransom as a sign of vulnerability or responsiveness to extortion. This perception could encourage the same ransomware operator or another one to attack that organization again or even lead the same attacker to demand more ransom for the same attack.

To learn more and create your free account, visit SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io