

Bridewell

Cybersecurity. *Where it Matters.*

RESEARCH REPORT 2024

Cybersecurity in US Aviation

Learn about the top cyber threats, trends and challenges facing aviation organizations in 2024.



Cybersecurity in Aviation

The civil aviation sector's high-profile role in the U.S. economy makes it an attractive target for cybercriminals and activists. The total reliance on thousands of different technologies and systems – many of which are entirely unique to the aviation sector – introduces many potential areas of susceptibility.

Aviation-related Internet of Things (IoT) covers a vast range of applications in air traffic control, passenger management, baggage handling, physical security and asset maintenance. The global IoT market in aviation, encompassing IT and OT, is set to grow by more than 23% each year up to 2030, according to Grand View Research. The U.S. market accounted for 35% of revenue in 2022. Growth will come from the proliferation of sensors, actuators and gateways for real-time data collection. AI and machine learning (ML) are also set to make a substantial impact in fields as varied as facial recognition, predictive and prescriptive maintenance.

“The global IoT market in aviation, encompassing IT and OT, is set to grow by more than **23% each year up to 2030**, according to Grand View Research.”



Key Threats and Challenges

Cyber threats are constantly developing. The research examined where the current threats are and how organizations in the civil aviation sector have reacted.



Protecting critical assets is the most frequently cited of the top five cybersecurity challenges in civil aviation – identified by **40% of respondents**. Managing cloud security (**31%**) and improving awareness and education (29%) are also challenges in this sector, along with supply chain risks (**29%**).



Over the previous 12 months, drone threats were the form of attack that U.S. civil aviation organizations most commonly experienced, with an average of **21 incidents**, according to respondents, compared with **18 incidents** of data theft or misuse, and **nine incidents** of unauthorized device use.



Accidental loss or disclosure of data is seen as the biggest risk to IT systems in the civil aviation sector (selected by **28% of respondents**), followed by malware (**26%**), and data theft or misuse (**24%**).



55% of civil aviation organizations experienced a ransomware attack over the previous 12 months. Of these, more than four-in-ten (**41%**) said that loss of data was one of the primary consequences. **38%** pointed to operational disruption. More than a quarter (**28%**) said the financial losses from paying a ransom were a consequence they had to deal with.

Key Threats and Challenges



For operational technology (OT) environments, the use of unauthorized devices is most often cited as a major risk **(31%)** followed by data theft or misuse **(24%)** and supply chain attacks **(22%)**. At the other end of the scale, only **10%** of respondents rated social engineering as a major risk, and **16%** said it was unpatched vulnerabilities.



Confidence in the protection of systems from cyber threats is relatively high in civil aviation – from **90%** expressing confidence in SaaS applications they use, and **84%** confident in their identity providers, to **81%** confident about their IT/OT boundaries.



This research also examined the speed of response to cyberattacks, which is critical to prevent further damage. While phishing attacks are dealt with in an average timeframe of **9.33 hours**, responses to ransomware take much longer **(16.81 hours)**. Responses to nation-state attacks take **13.79** hours on average. Although this is faster than for ransomware, nation-state threats must be a concern for the aviation industry, due to its high profile.



Looking Ahead

The research also looked at what is likely to shape cybersecurity in civil aviation over the next 12 months.

When examining the most serious threats to operations throughout 2024, it is 5G network vulnerabilities that attract the highest percentage of respondents **(28%)**, followed by insider threats, cloud storage attacks and attacks on automated technologies (all named by **26%** of respondents). Social engineering and phishing were much lower **(10%)**.

The potential event or nation-state threat that worries more civil aviation respondents than any other is from China. **90%** of respondents said they are concerned about state-linked actors in China, compared with **79%** worried about similar threats from Russia. More than three-quarters **(76%)** cite concerns about the U.S. presidential election in November, but more **(81%)** are worried about disruption from economic turbulence or another global health crisis **(83%)**.

“ The potential event or nation-state threat that worries more civil aviation respondents than any other is from China. ”

AI

AI is obviously a major area where threats are evolving as criminals learn how to utilize AI tools within their attacks. There are many types of AI-driven threats and the civil aviation industry is concerned about all of them – from the 90% worried about AI-powered phishing and automated hacking, to the 79% concerned about polymorphic malware (malware that can adapt itself for greater impact) and the 78% fearful of AI-powered botnets.

AI also has immense potential to protect systems and data. Almost every organization surveyed (98%) is using at least one AI-driven tool such as AI-enhanced endpoint protection, automated incident response solutions, or network behavior analysis. The most popular tools are SASE (secure access service edge) solutions and deep learning for malware analysis – adopted by 31% of respondents.



“ There are many types of AI-driven threats and the civil aviation industry is concerned about all of them. ”

The Changing Regulatory Landscape

The Transportation Security Administration (TSA) security directives introduced in March 2023 require airport and aircraft operators to develop an approved implementation plan that describes measures they are taking to improve their cybersecurity resilience and prevent disruption and degradation to their operational technology (OT) and IT infrastructure. The directives were broadened to protect higher-risk rail and bus transit. An update to the TSA Security Directive also aims to reinforce cybersecurity preparedness and resilience for critical pipelines in the U.S.

New requirements are designed to prevent occurrences such as the attack on Long Beach Airport which affected their website and payment processing. They focus on network segmentation, access control, monitoring and detection and patch management.


All civil aviation organizations surveyed have started preparations for the TSA regulations. 47% have everything in place, while 43% are almost where they need to be. Just 10% still have a long way to go.

Steps taken include strengthened incident response and reporting, improved training and education, and the use of wider industry expertise (all among the top five compliance tactics selected by 28% of respondents).

In addition, the research asked what measures organizations have introduced as a result of President Biden's National Cybersecurity Strategy.

The strategy, introduced in 2023, has five pillars, the first of which is to defend critical infrastructure. This includes expanding the use of minimum cybersecurity requirements and the harmonization of regulations to reduce compliance burdens.

The top five measures taken by civil aviation respondents in response to the National Cybersecurity Strategy include incident reporting, business continuity management, staff training and awareness raising (all selected by 28% of respondents). Incident response and recovery plans are less popular (16%).



“ All civil aviation organizations surveyed have started preparations for the TSA regulations. ”

Budgets, Spending and Skills

Spending on cybersecurity by civil aviation respondents' employers is well above the average across all U.S. sectors surveyed for Bridewell. This research indicates that the average percentage of IT budgets critical infrastructure organizations spent on cybersecurity is 45%, compared with 54% in the civil aviation sector.

Civil aviation respondents will also spend an average of 52% of their OT budgets on cybersecurity, compared with an average of 42% across all the critical infrastructure organizations surveyed. In terms of revenue, respondents say 48% is spent on cybersecurity on average in civil aviation, compared with a critical infrastructure overall average of 42%.

Most civil aviation organizations are increasing investment in cybersecurity. Over the next 12 months, the research found 72% will spend more on IT security than they did in 2023, while 16% will spend less. More than a quarter (26%) of respondents' organizations will spend less on OT security in the coming year, but 67% will spend more.

The cyber skills shortage is a global problem, and in the U.S., civil aviation organizations are adopting a range of measures, with the funding of STEM programs at universities being the most popular (38%) followed by outsourcing, reskilling, employee recommendation apprenticeship programs and contact with regional security organizations (all 34%).



“ Most civil aviation organizations are increasing investment in cybersecurity. ”

How Does the Civil Aviation Sector Compare to Other Critical Infrastructure Sectors?

These findings show that while the emphasis may vary, there are common threads across the critical infrastructure sectors surveyed.

Phishing and malware, for example, remain potent threats, along with ransomware. All sectors, with the exception of road transportation, continue to be under attack from ransomware gangs.

The figures show 55% of civil aviation organizations experienced a ransomware attack, along with 78% of financial services, 76% in the rail sector, 71% in federal government organizations, and 60% in the energy sector. By contrast, only 29% in the road sector experienced the attention of criminals using ransomware.

Data loss and theft are major concerns, with organizations fearful of losing intellectual property and other vital data, along with the high risk of infringing data privacy laws. Many organizations also appear to have paid ransoms despite the risk of transacting with sanctioned entities and the potential for severe penalties.

Speed of response to incidents, which is important for the reduction of damage, varies according to attack type and sector. Federal government organizations are faster than the critical infrastructure average, for example. On average they take less than six hours to respond to a supply chain attack compared with an average of more than 12 across all sectors surveyed in this research. Another exception is road transportation where organizations respond to nation-state attacks in about three hours, compared with the 27 it takes to respond to drone threats.

Road and rail sectors are less worried about terrorist and nation-state attacks than most, but each sector has its own concerns. Rail respondents are particularly worried about the security of 5G networks over the coming 12 months, for example. In federal government organizations there were significant concerns about the need to improve cyber awareness and education. Social engineering is an area for them to focus on. Despite suffering more social engineering attacks than any other type of attack, only 16% of organizations in the federal government category regard social engineering as among the most serious threats to their IT environments.



How Does the Civil Aviation Sector Compare to Other Critical Infrastructure Sectors?

All sectors, however, demonstrate widespread confidence in the protection of their OT and IT systems, even if too few respondents view terrorist and nation-state cyber activities as the dangers they are. This is particularly noticeable among energy sector respondents.

AI is a hot technology and high percentages of respondents, especially in financial services, are concerned about AI threats such as adaptive attacks. It may be easy to attribute this to the deluge of public debate on the topic, but there is no doubting that AI is a major force in cybersecurity – for good as well as bad. The vast majority of organizations surveyed here already use one or more AI-based tools to reinforce their cyber defenses, which is encouraging.


While efforts to comply with regulations such as the TSA and NCS are generally well-advanced, there are still too many organizations planning to cut expenditure on IT and OT security. They are in a minority, but at a time of heightened international tension and activity from state-affiliated cyber gangs, this may turn out to be fatally short-sighted.

Overall, we have a picture of critical infrastructure organizations that have a good eye for compliance but are advancing towards cybersecurity maturity at different speeds. With a continuing shortage of cybersecurity talent, organizations need to ensure they have as much access to expertise as possible.



Bridewell

Cybersecurity. [Where it Matters.](#)

 +1 713 300 4009

 hello@bridewell.com

 bridewell.com