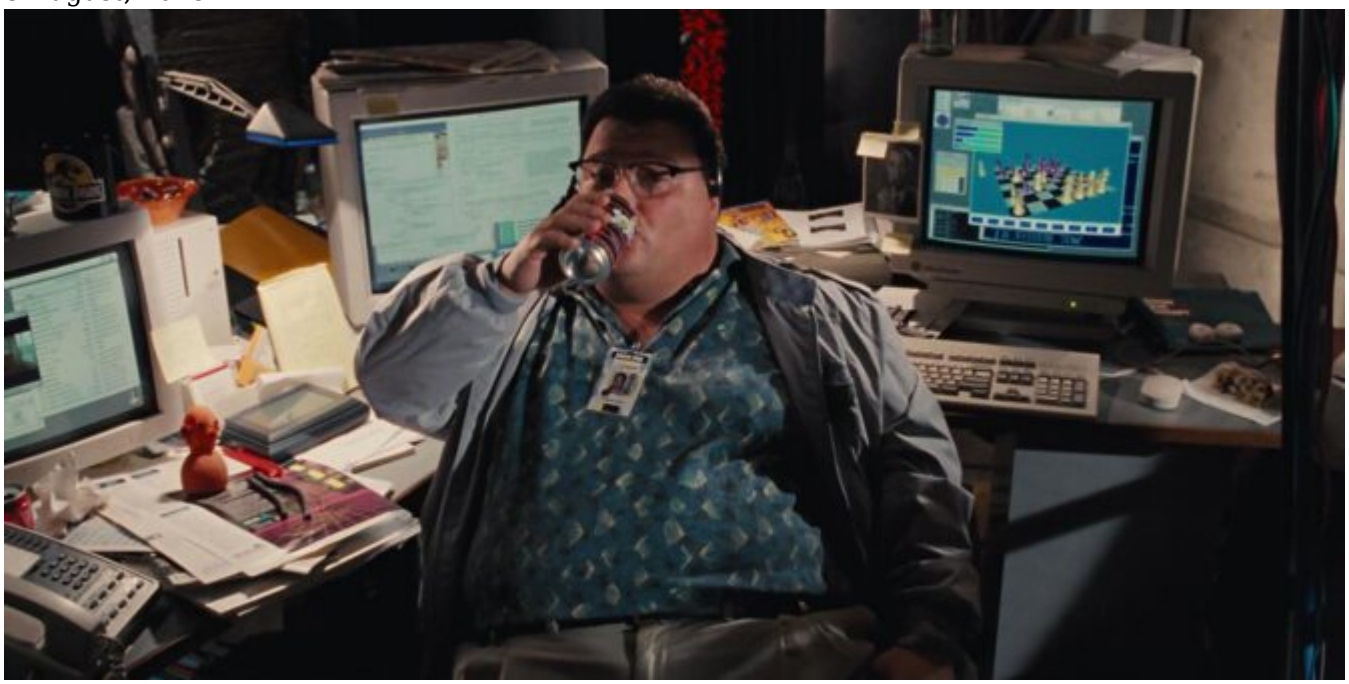
Cybersecurity in Aviation: Growing Operational Risk

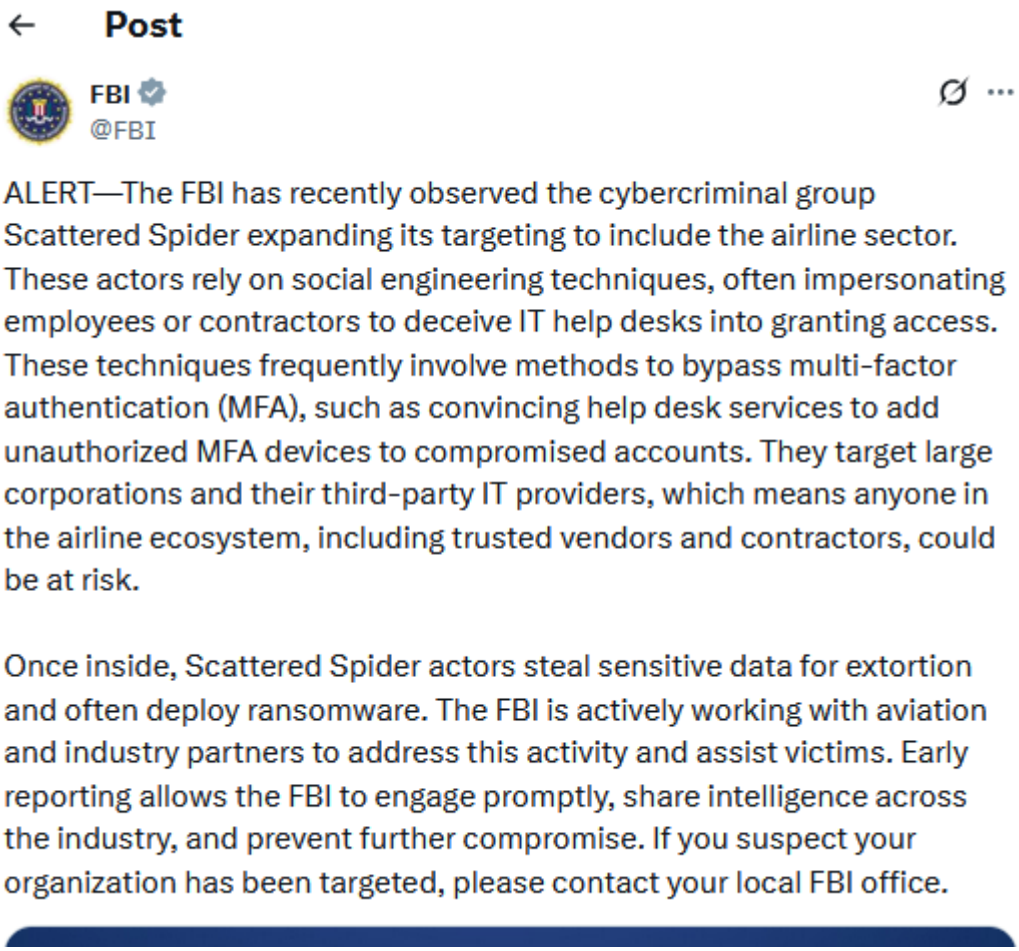
Chris Shieff
5 August, 2025



Aviation is under fire

A recent study recorded a 600% increase in attacks on the aviation sector year-on-year. 71% of these involved credential theft or unauthorised access to critical systems.

The FBI also warned on June 28 that a cybercriminal group called ‘Scattered Spider’ had turned its attention toward the aviation sector, using impersonation to compromise security.



The alert was issued on X.

Protecting ourselves from these attacks has become a **multi-million dollar** industry.

High profile attacks in recent months have impacted both Aeroflot and Qantas, the latter likely carried out by none other than Scattered Spider – the group the FBI are worried about.

The FAA is paying attention

There has been a response to this growing risk.

There is an obvious intent to **include cyber security in future regulations.** While not yet law, recent advisories and bulletins make it clear that operators are expected to begin taking proactive steps.

A good place to start is AC 119-1A which provides an overview of cyber security requirements, risk assessments and best practices. Also keep an eye out for cyber threat alerts which can be published by SAFO, Notam or other notices.

The FAA is also actively working with ICAO and other agencies to **harmonise future cyber protection practices** under Annex 17 (Security).

What about business aviation?

The examples above relate to attacks on larger airlines and IT infrastructure. A valid question remains then, what does this all mean for biz av?

While not a traditional target, many business aviation operators **lack dedicated IT departments or cyber defence teams.** We also frequently carry high-net worth individuals on sensitive operations which

may motivate nefarious cyber activity.

Recent reports from the industry show that biz av isn't immune:

In 2020, a major manufacturer of business jets confirmed a cyber-security breach that compromised personal and aircraft ownership information.

Another example from May this year involved a Europe-based private jet operator which appeared on a ransomware group's leak site. Sensitive crew info was shared, which reportedly included passport photos.

It's clear that business aviation is **not under the radar** – therefore we must remain measured but cautious in our approach to emerging cyber threats.

EFBs – A Soft Target?

Feedback from industry experts and OPSGROUP members suggest that a closer look at the electronic security of EFBs warrants a **closer analysis.**

The role of EFBs in cyber crime warrants a closer analysis.

Eye-opening research, such as the work conducted by Cyber Security Consultancy Pen Test Partners, has highlighted that EFBs could act as an additional gateway for cyber crime if not **correctly managed.**

Look out for an dedicated article on this subject soon.

An extra tip – don't forget your SMS

If your flight department operates under an SMS, it may be wise to include cyber security.

This means treating digital threats like any other hazard – **reportable, measurable and mitigable.**

It's important we take steps now to keep our operations secure.