The Day the Aircraft Couldn’t Leave the Gate

(Information Security: Part 1)

On June 21, 2015, LOT Polish Airlines experienced something unusual.

Aircraft were ready.

Crews were in position.

Weather was not a factor.

And yet—nothing moved.

A cyberattack targeted the airline’s ground-based flight planning system. Specifically, a distributed denial-of-service (DDoS) attack overwhelmed the system that generates flight plans.

Without a valid flight plan, aircraft could not legally depart.

The result:

- Over 1,400 passengers stranded
- Dozens of flights delayed or canceled
- An airline temporarily grounded—not by weather, not by maintenance, but by **data disruption**

This Wasn't an IT Failure—It Was Operational Paralysis

It's easy to hear "cyberattack" and think:

That's an IT issue.

But what actually happened?

- Dispatch couldn't generate flight releases
- Crews couldn't receive required operational data
- Aircraft couldn't move safely or legally

This wasn't a technology inconvenience.

It was a **complete breakdown in operational capability**.

👉 The system failed in the same way a critical aircraft system might fail.

👉 And the operation responded the same way—by stopping.

Information Is Safety-Critical

In aerospace, we're trained to think of safety in physical terms:

- Aircraft systems
- Weather conditions
- Pilot performance

But modern operations depend on something less visible:

Information.

Flight plans.

Weight and balance data.

Weather inputs.

Maintenance records.

Safety reports.

If that information is:

- **Unavailable**
- **Corrupted**
- **Delayed**
- **Untrusted**

Then decision-making is compromised.

And when decision-making is compromised, **safety is already degraded.**

A New Kind of Human Factors Risk

We already understand threats like:

- Fatigue
- Distraction
- High workload
- Communication breakdowns

Now consider this:

What happens when a crew or dispatcher is working with **incomplete or unreliable data**?

- Increased cognitive load
- Delayed decisions
- Conflicting information
- Erosion of trust in systems

Sound familiar?

That's not an IT issue.

That's **human factors under degraded conditions**.

👉 Cyber disruption doesn't just attack systems—it attacks **decision-making environments**.

The Risk You Can't See

The most dangerous part of information security risk is this:

You often don't know it's happening.

Unlike a system failure, there may be:

- No warning light
- No immediate indication
- No obvious failure mode

The data may simply be… wrong.

Or missing.

Or delayed just enough to matter.

And decisions continue to be made.

Why This Matters to Safety Management Systems

Safety Management Systems (SMS) are built on one critical assumption:

👉 **The data is accurate, complete, and trusted.**

Think about what your SMS depends on:

- Voluntary safety reports
- Risk assessments
- Trend analysis
- Safety performance indicators

If the integrity of that data is compromised—even slightly—your entire safety picture becomes distorted.

You may:

- Miss emerging risks
- Misjudge severity
- Make decisions based on incomplete information

WYVERN Perspective

Because WYVERN provides support, services, and products to aerospace organizations around the globe, we often say, **“We don’t fly aircraft—we fly data.”**

Data integrity is fundamental to everything we do—and we are committed to safeguarding the data our clients trust us with, which is why we implemented ISO 27001 standards and recommended practices to ensure information security.

ISO 27001 principles include data *confidentiality, integrity, and availability*, which are critical to every organization’s success. For example:

- Your SMS must include specific confidentiality features
- Your safety culture depends on data integrity
- Your decision-making depends on data availability

👉 **While ISO 27001 provides the framework for security, its true value is realized in day-to-day operations—where data integrity directly supports operational safety.**

A Shift in Mindset

Information security is no longer:

- A compliance checkbox
- A background IT function
- Someone else’s responsibility

It is:

👉 A **dispatch issue**

👉 A **flight-line issue**

👉 A **leadership issue**

👉 A **safety issue**

Looking Ahead

In Part 2, we’ll break down:

Where aerospace systems are most vulnerable—and what that means for your operation.

Because the first step is recognizing the risk.

The next step is understanding **where it lives.**

Closing Thought

If your operation depends on information to make safe decisions…

Then protecting that information isn't IT.

It's safety.

Subscribe to our newsletters now at the bottom of this page. For further resources and guidance on implementing Safety Management Systems, contact WYVERN, THE industry expert. Attend our **SMS Training Workshops** or ask about our SMS software. **Contact us for a FREE SMS demo**! Together, we can elevate aerospace safety and create a safer future.

References

- Civil Aviation Authority. *Cybersecurity in Aviation (CAP 1753)*.
- European Union Aviation Safety Agency. *Easy Access Rules for Information Security (Part-IS)*.
- Federal Aviation Administration. *Safety Management System (SMS) Framework (AC 120-92B)*.
- International Air Transport Association. *Cyber Security Toolkit & Guidance for Aviation*.
- International Civil Aviation Organization. *Annex 19 — Safety Management*.
- International Civil Aviation Organization. *Aviation Cybersecurity Strategy (Doc 10101)*.
- LOT Polish Airlines DDoS attack 2015.