

The Day the Data Lied



The Day the Data Lied

No warning. Just the wrong information.

When Information Breaks Down: The Operational Impact of Data Disruption

The “Silent Failure”

In Part 1, we discussed why information security matters. Here, we focus on what happens when that system begins to fail—often in ways that are not immediately obvious.

On August 3, 2016, Emirates Flight 521 was on approach into Dubai.

The conditions were challenging but manageable. The aircraft touched down, and the crew initiated a go-around.

But something didn’t respond as expected.

The aircraft’s system logic indicated that the wheels were still on the ground—just long enough to prevent the automated go-around from activating.

The crew executed the correct action.

The system, based on its data, did not.

There was no clear indication that the command had not been accepted.

No warning.

No immediate feedback.

Just a growing mismatch between what the crew believed the aircraft was doing—and what it was actually doing.

By the time the discrepancy became clear, the aircraft had lost critical energy.

What followed is often discussed as a handling event.

But underneath it was something more subtle:

A moment where **data, timing, and system logic were no longer aligned.**

What Information Failure Really Looks Like

In a mechanical failure, you get a warning.

A Master Caution. An annunciation. A clear signal that something is wrong.

But in an information failure, it is often different.

You may get no warning at all.

Or worse—

You may get a “green light” for the wrong information.

The “Silent Failure” in Daily Operations

These breakdowns are rarely dramatic.

More often, they look like this:

- A delayed weather uplink
- A mismatch between dispatch and onboard routing
- Maintenance records that don’t fully reflect the aircraft’s status

Individually, these issues seem manageable.

Together, they create something far more dangerous:

Uncertainty.

The crew begins cross-checking. Dispatch is called. Maintenance is consulted.

Time pressure builds.

What should have been routine becomes complex—before the aircraft ever leaves the ground.

When Information Breaks Down

1. Task Saturation Increases

When systems don't align, people compensate.

- Flight crews manually verify
- Dispatch rechecks data
- Maintenance confirms records

Automation gives way to manual processes.

Workload increases—not from failure, but from **friction**.

This is how task saturation begins.

2. Conflicting Information Erodes Trust

When systems disagree, confidence degrades.

- Flight plan vs. FMS
- Weather application vs. ATIS
- Maintenance record vs. aircraft condition

The question shifts from “*What is the plan?*” to:

“Which version of the truth is correct?”

And that hesitation introduces risk.

3. Situational Awareness Degrades

Situational awareness depends on information that is:

- Correct

- Consistent
- Usable in the moment

When any of these break down, the operational picture becomes incomplete.

Teams are no longer operating with clarity—

They are operating with gaps.

4. Decision-Making Becomes Reactive

Instead of staying ahead of risk, teams begin to:

- Verify instead of execute
- Catch up instead of anticipate
- Manage uncertainty instead of manage operations

This is where small disruptions begin to compound.

And where operational resilience starts to erode.

When Data Degrades, Safety Systems Follow

This is not simply an IT issue.

It is a **Safety Management System issue**.

When data is degraded, your SMS does not fail outright—

It quietly becomes less effective.

- Hazards may go unrecognized
- Trends may be missed
- Decisions may rely on incomplete inputs

As outlined by the International Civil Aviation Organization and reinforced by the Federal Aviation Administration, safety management depends on the integrity, availability, and reliability of operational data.

Without it, even strong systems begin to weaken.

Looking Ahead

If the operational risk is clear, the next question becomes:

Where does the breakdown actually begin?

Legacy safety training and current accident investigation techniques still focus too much on human error as causal.

In reality, it is often a symptom of a systems breakdown—such as recruiting, training and qualification, and management oversight.

Coming Next

In Part 3, we will explore:

- How social engineering targets aviation professionals
- Why the human layer is often the most vulnerable
- What cyber hygiene looks like in real-world operations

Because protecting information is not just a technical challenge—
It is a human one.

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

- International Civil Aviation Organization. *Safety Management Manual (Doc 9859)*.
- Federal Aviation Administration. *Advisory Circular 120-92B: Safety Management Systems for Aviation Service Providers*.
- European Union Aviation Safety Agency. *Easy Access Rules for Air Operations*.
- National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*.

- International Organization for Standardization. *ISO/IEC 27001: Information Security Management Systems*.
- Safety Management International Collaboration Group. *Safety Culture Evaluation Tool*.
- Flight Safety Foundation. *Safety publications and resources*.