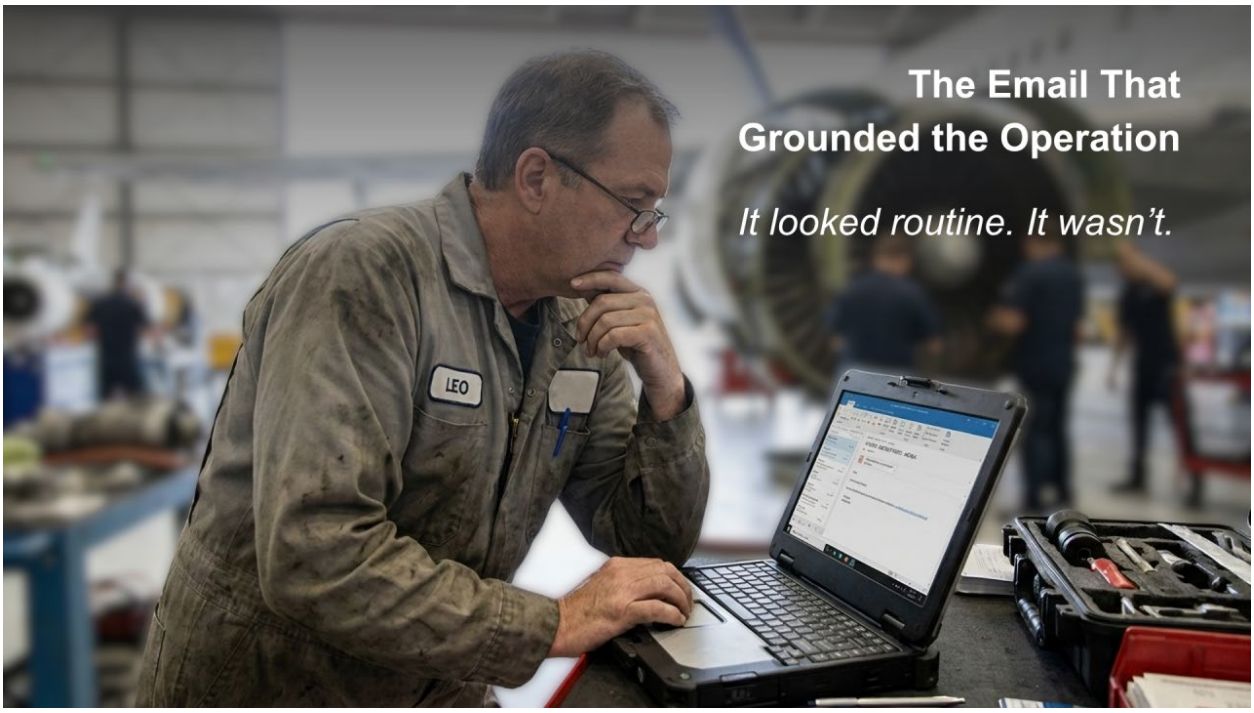
The Email That Grounded the Operation



When the Human Layer Becomes the Target

It looked routine.

An email from a known vendor.

A simple update—new banking details for an upcoming payment.

The timing aligned. The formatting was correct.

Nothing raised concern.

The payment—over $150,000—was sent.

The parts never arrived.

What followed was not just a financial loss, but operational disruption.

A critical aircraft was grounded for weeks while the issue was resolved.

The email address had been altered by a single character.

This is not an isolated event.

According to the Federal Bureau of Investigation Internet Crime Complaint Center (IC3), Business Email Compromise has resulted in **billions of dollars in annual losses**

worldwide, with high-value industries like aerospace frequently targeted due to the size and urgency of transactions.

Where the Breakdown Actually Begins

In Part 2, we explored what happens when information begins to degrade. But often, the breakdown begins earlier—before incorrect data ever enters the system.

This is where **Social Engineering** comes into play.

Social Engineering attacks do not target systems first—they target people. They exploit human psychology rather than technical vulnerabilities, manipulating individuals into taking actions that compromise security. Instead of hacking systems directly, attackers build trust, create credibility, and persuade their target to share sensitive information, click malicious links, or approve unauthorized actions.

These attacks are rarely random. They are researched, intentional, and designed to feel legitimate. An attacker may study publicly available information, understand operational context, and impersonate a trusted individual—such as an executive, a vendor, or a member of maintenance control. The request is then delivered through familiar channels—email, phone, or messaging—often with a sense of urgency that discourages verification.

By the time the interaction occurs, the groundwork has already been laid. The message fits expectations. The timing makes sense. The tone feels right.

And it works because it exploits well-known human tendencies:

- **Expectancy Bias** — we see what we expect to see
- **Plan Continuation Bias** — we continue despite subtle inconsistencies
- **Authority Bias** — we are inclined to comply with perceived authority

The request looks right. The context makes sense. It appears to come from the right person. So, the action is taken.

What Social Engineering Looks Like in Aerospace

Spear Phishing

Highly tailored messages directed at specific individuals or operations.

- Referencing a real tail number

- Mentioning an actual trip or destination
- Mimicking known vendors or internal personnel

Business Email Compromise (BEC)

Manipulating legitimate communication threads to redirect payments or sensitive data.

Credential Harvesting

Replicating trusted systems to capture login credentials.

Why Aviation Is Especially Vulnerable

Aviation environments create ideal conditions for these threats:

1. **Time Pressure:** Decisions are made quickly. Urgency reduces the instinct to question.

2. **Distributed Operations:** Teams operate across locations, systems, and time zones. Verification is not always immediate.

3. **High-Trust Culture:** Professional trust is essential—but it can also be exploited.

4. **Complex Information Flow:** Multiple systems and communication channels increase the potential for inconsistency.

5. **Authority Gradient:** Aviation professionals are trained to respect the chain of command. Instructions from leadership, maintenance control, or flight operations are often acted on quickly—by design.

Attackers exploit this through authority bias:

- Impersonating a Director of Maintenance
- Spoofing an executive request
- Framing messages as urgent directives

The request feels legitimate because it follows the expected chain of command.

How the Risk Unfolds

The progression is subtle.

It begins with a request that feels routine, something that aligns with expectations and does not immediately raise concern. Because it looks right and arrives in the right context, it is accepted without hesitation.

From there, incorrect information is introduced. The system itself is not compromised; rather, it is quietly misinformed. The data appears valid, so it continues to move through the operation unchecked.

As a result, operations begin to drift. Confusion builds, time pressure increases, and teams start compensating for small inconsistencies without fully recognizing their source. What seems manageable in the moment gradually becomes more complex.

Eventually, a “silent failure” emerges. There is no alert and no clear point of breakdown—only a widening gap between what is believed to be true and what actually is.

This Is a Safety Issue

This is not simply cybersecurity. It is operational risk.

Organizations like the International Civil Aviation Organization and the Federal Aviation Administration emphasize that safety depends on:

- Accurate information
- Reliable communication
- Shared understanding

Social Engineering disrupts all three—Without ever touching the aircraft.

Standards such as ISO 27001 provide the framework, while ISO 27002 outlines specific controls for human behavior, verification, and information handling.

Protecting information is not just a technical exercise—It is an operational one.

What Cyber Hygiene Looks Like in Practice

This is not about adding complexity. It is about applying aviation discipline to information handling.

Standardize Verification: Treat changes in critical data—such as banking details or credentials—as a required cross-check.

Challenge the Urgency: In aviation, *fast is slow*. Requests that demand immediate action should be treated as potential red flags.

Pause and Reassess: If something feels slightly off, stop and verify before proceeding.

Report Early Signals: Small inconsistencies are often the first indicators of a larger issue. These are not IT controls. They are **operational safeguards**.

WYVERN Perspective

Information does not become risk on its own. It becomes risk in how it is accepted, interpreted, and acted upon. In aerospace, decisions are made in dynamic environments—where time is limited, information is flowing, and trust is often assumed.

That is where vulnerability begins.

A strong Safety Management System must account for more than systems and data:

It must account for how people:

- Recognize what doesn't look right
- Respond to unexpected inputs
- Verify before they act

Because even accurate systems can be undermined by incorrect assumptions—And even small breakdowns in judgment can introduce operational risk. In today's environment, the most significant vulnerabilities are not always technical. They are human.

Final Thought

The question is no longer**: *"Are your systems secure?"***

It is**: *"How does your team respond when a request for sensitive and critical information appears slightly off?"***

Because in aerospace, risk does not always arrive as a failure.

Sometimes—It arrives as an expected and reasonable request.

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*.
- International Organization for Standardization. *ISO/IEC 27001 Information Security Management Systems*.
- International Organization for Standardization. *Code of Practice for Information Security Controls*.
- Federal Bureau of Investigation. *Internet Crime Complaint Center (IC3) Reports*.
- National Institute of Standards and Technology (NIST). *Cybersecurity Framework*.
- Flight Safety Foundation. Safety publications and resources.