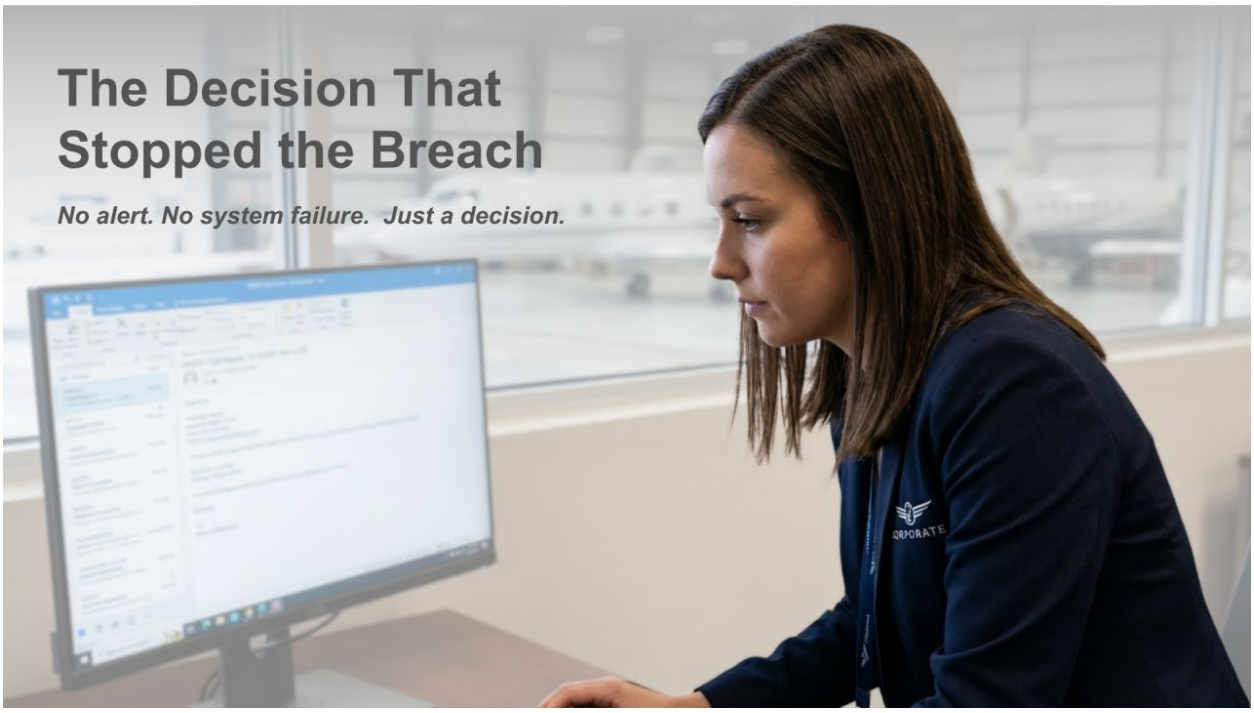
The Decision That Stopped the Breach



A message arrives.

It appears to come from a trusted source—a regulator, a vendor, or an internal department.

A familiar name. A simple instruction to review a “mandatory update.”

The kind of message that fits seamlessly into normal operations—and moves things forward without hesitation.

In recent years, aviation professionals have been increasingly targeted by messages like this—crafted to blend into the flow of daily work.

But in some cases, a team pauses. Not because the system blocks the message—but because something doesn’t fully align.

The tone doesn’t match. The urgency feels misplaced. The link doesn’t align with the sender’s domain.

So they verify it.

Not by clicking—but by cross-checking through official channels.

What they uncover is not a routine update, but a credential harvesting* attempt designed to gain access to operational systems.

What could have become a data breach—or an operational disruption—stops before it ever enters the system.

No alert. No system failure. Just a decision.

Credential harvesting—sometimes called credential phishing—is when an attacker attempts to collect login information, such as usernames, email addresses, and passwords, by presenting something that appears legitimate. Instead of breaking into a system directly, the attacker relies on someone to unknowingly provide access. Once obtained, those credentials can be used to enter operational systems, access sensitive data, or initiate further actions within the organization.

What Went Right

In Part 1, operations stopped because systems were unavailable.

In Part 2, risk emerged because data could not be trusted.

In Part 3, the threat entered through people without ever touching a system.

Here, none of that happened. Because someone noticed. Not a major red flag. Not a system warning. Just a subtle inconsistency. And more importantly, they felt empowered to act on it.

This Is What Resilience Looks Like

We often define security by what systems prevent.

Firewalls. Access controls. Authentication layers.

But in real-world operations, risk is often stopped somewhere else—

In the moment a person decides to question what doesn't fully align.

- When something that *looks right* is still challenged
- When urgency does not override judgment
- When verification happens before action

This is not hesitation. This is operational discipline.

From Vulnerability to Control

For years, cybersecurity discussions framed people as the weakest link.

But more recent guidance has shifted that perspective.

The National Institute of Standards and Technology Cybersecurity Framework (updated in 2024) emphasizes that human behavior is not simply a risk to manage—it is a critical component of defense.

Similarly, International Civil Aviation Organization's aviation cybersecurity strategy (Doc 10101, reaffirmed in recent updates) highlights that cyber resilience depends on integrating human factors into security practices—not separating them from it.

In other words:

The same human layer that can be exploited— is also the layer that can stop the threat entirely.

The Real Control

In aerospace, this isn't new.

We verify, cross-check, and challenge inconsistencies— not because we expect failure, but because we're trained not to assume correctness.

The difference now is context.

The same discipline that protects flight operations is what protects information.

Technology will evolve—and so will the threats.

But the most reliable control remains the one closest to the decision:

The individual who pauses and verifies— not because a system requires it, but because the culture promotes and supports it.

The message looked right. The system didn't stop it.

But the operation didn't fail because someone chose to verify.

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

- National Institute of Standards and Technology (2024). *Cybersecurity Framework (CSF) 2.0*.
- International Civil Aviation Organization (2022). *ICAO Aviation Cybersecurity Strategy (Doc 10101)*.
- Cybersecurity and Infrastructure Security Agency (2023–2024). *Phishing and Social Engineering Guidance*.