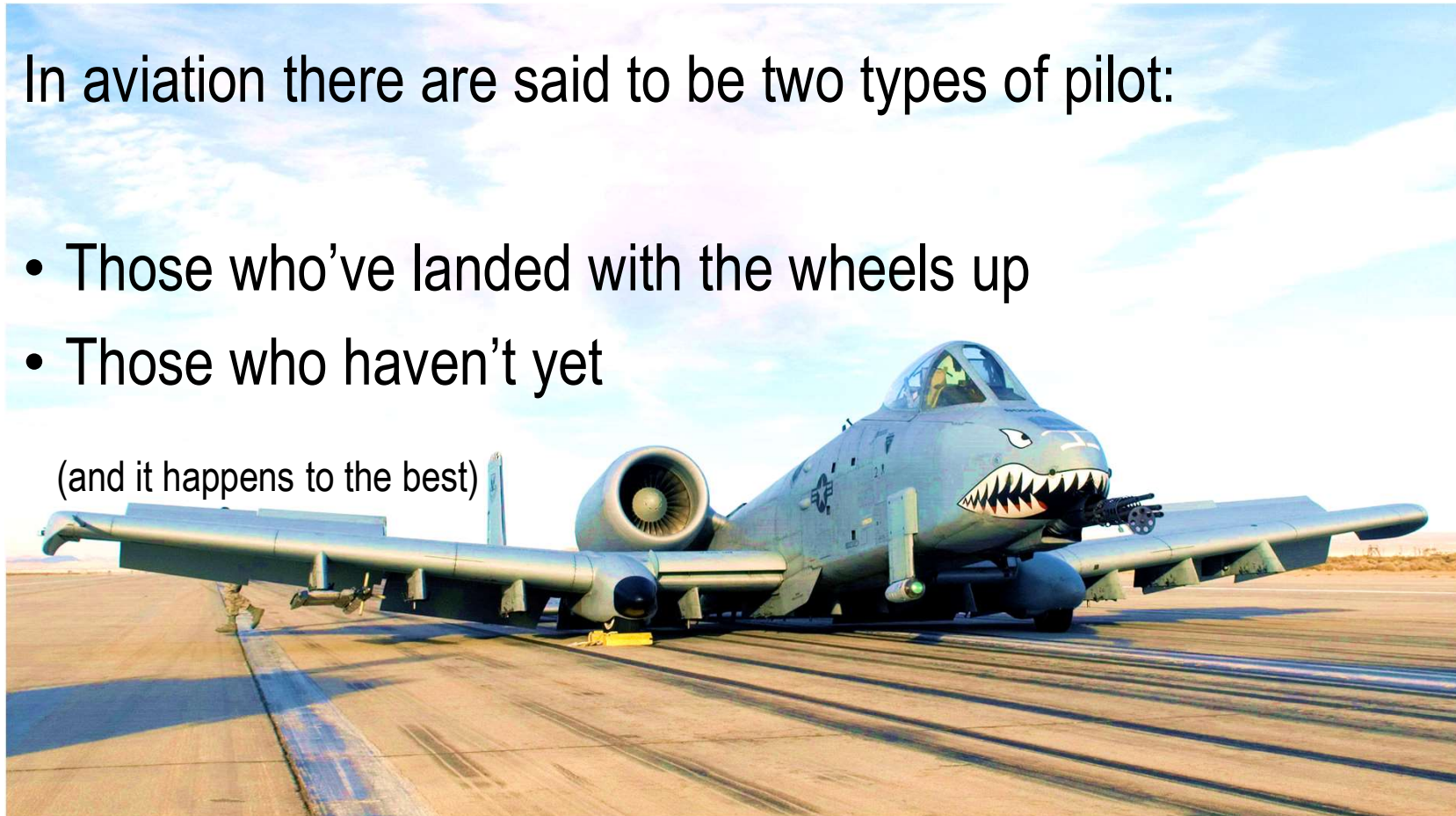# Taking a risk-based approach to cyber security

When, not if

In aviation there are said to be two types of pilot:

- Those who've landed with the wheels up

- Those who haven't yet

(and it happens to the best)

Your systems <u>are</u> under attack

Ever…

• receive phishing emails?

• get unexpected calls claiming to be from a supplier?

• notice strange transactions on your bank statement?

Your company is also being targeted

Risk?

Aim to **manage risk** rather than 'secure' your systems

- You have limited resource, use it wisely

- Direct your action towards the largest risks

- There will be low-hanging fruit – pick it!

- Knowing <u>what</u> you have is the first step

How? (high-level, not at all a comprehensive plan of action)

1. Define the system you need to protect

2. Create an asset register

3. Research threats and vulnerabilities

4. Assess the risk posed by loss or misuse of each asset

5. Make the most cost-effective mitigations

6. Repeat

Spoiler alert!!!

Unless you already have a comprehensive Cyber Security Management System in place…

The most cost-effective mitigations to address your biggest risks are **not** likely to be high technology Intrusion Detection and Protection Systems

Activities such as…

Educating staff

To what phishing emails might look like

Educating staff

To format USBs using a dedicated machine before use

Updating and password protecting

The engineering laptop that's used by everyone, including contractors

https://www.flickr.com/photos/jemimus/6461569529

Even the last person to leave...

Locking all the doors and windows

https://www.flickr.com/photos/dahlstroms/4511228299

Will have a much greater impact

And…

- Cost significantly less

- You can start today

- You can start now

- Start now:

<div align="center">

0161 660 4293

richard@op-tec.co.uk

</div>