BT Group

Practical Secure by Design

Driving security as a core business requirement

Dean Taylor, Senior Manager, Security Consultancy Practice

April 2024

Work:

8 years as an Electrical Engineer

12 years in IT and Networks

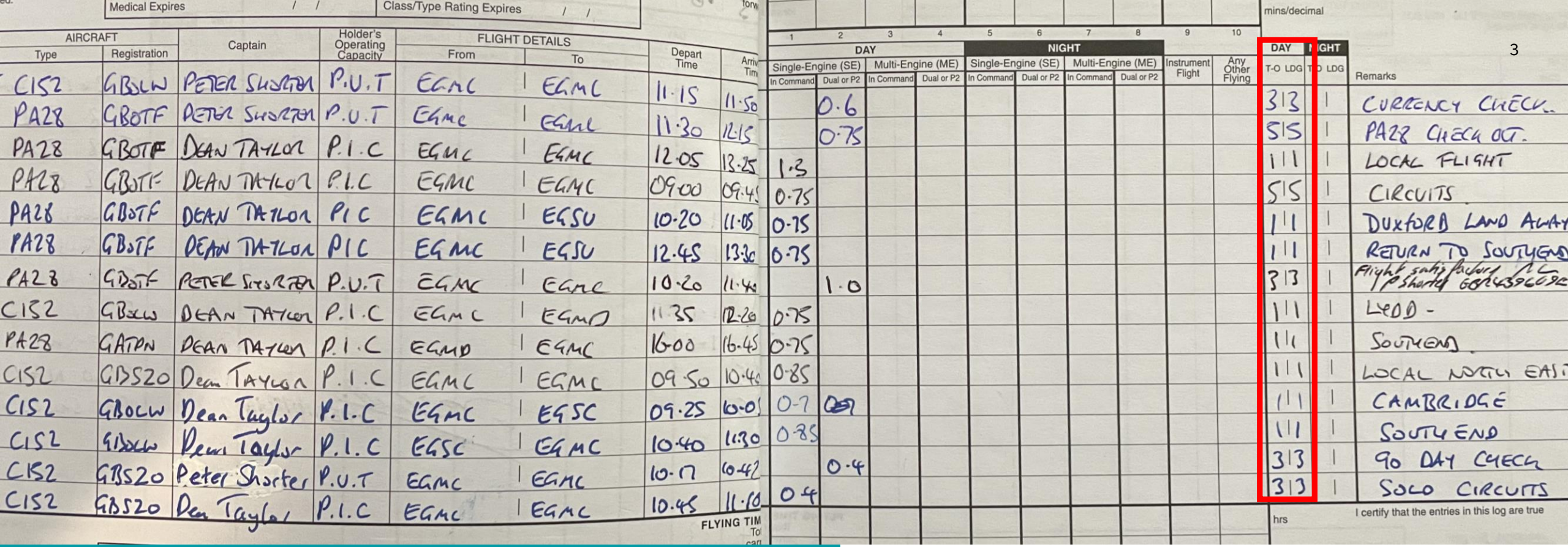
12 years in Cyber Security

Currently lead the Security Consultancy practice

Play:

A passion for computing and tinkering

A passion for making things fly or flying in things

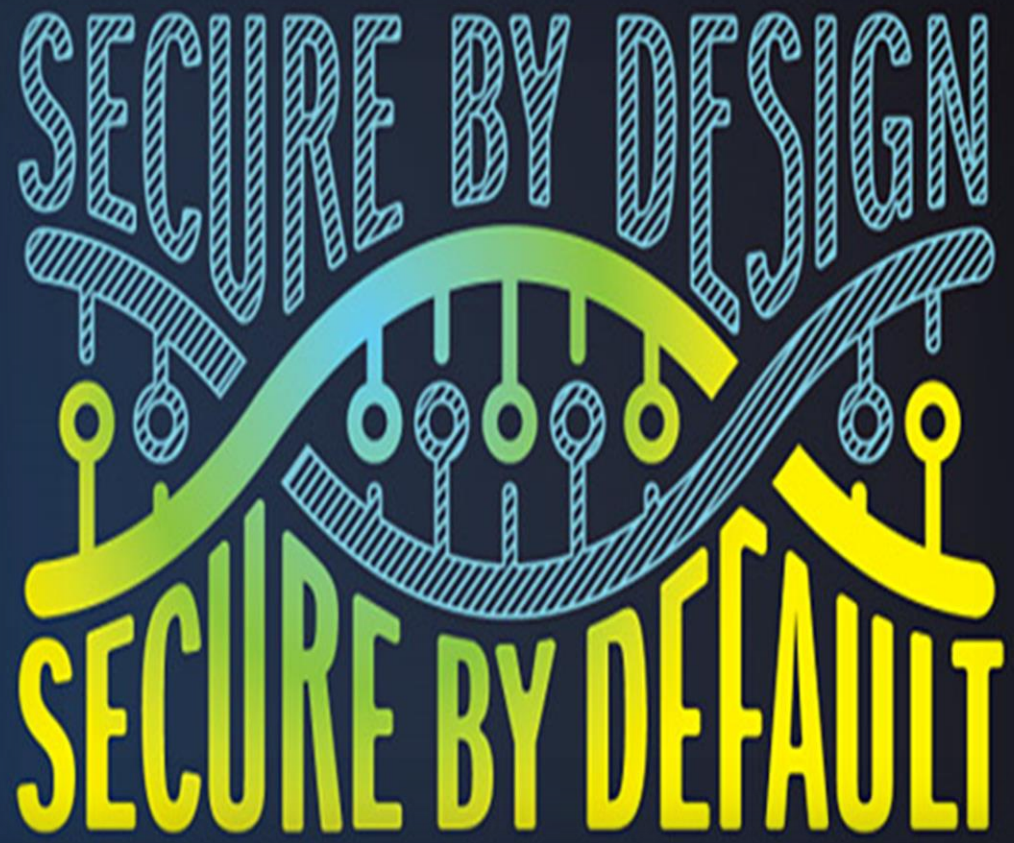


consistency = knowledge + skill + luck
(luck = preparation + opportunity)

Success = landing the same number of times as you take off

Failure = when you run out of skill and luck

To be consistent you first need goals



"Get the right security designed in early before it's too late to make a difference"

"Ensure the default configuration is the most secure settings possible"

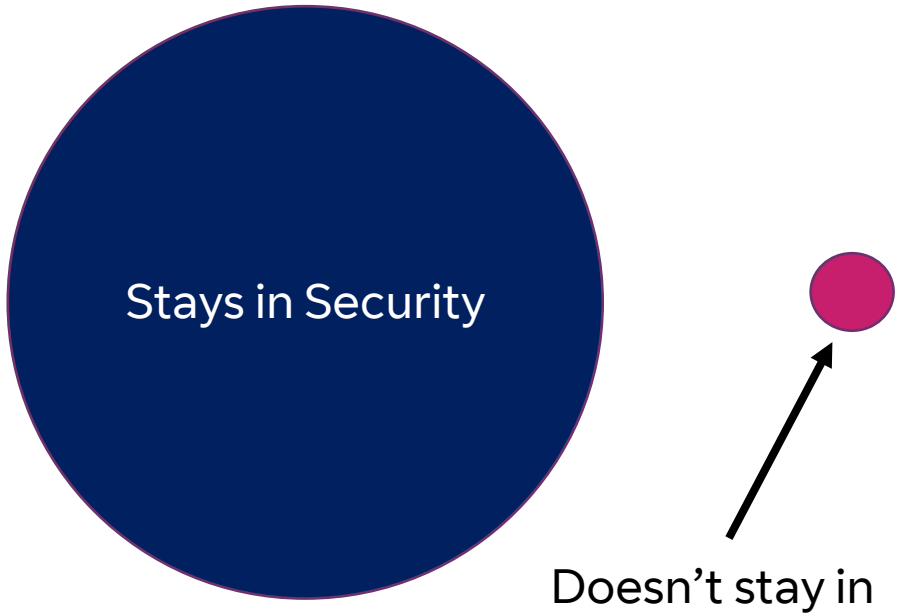
How it began...

- No process
- No tooling
- We lacked credibility
- Reactive
- Complete chaos
- Our reality: Contain it or watch it blow up

Early Mistakes

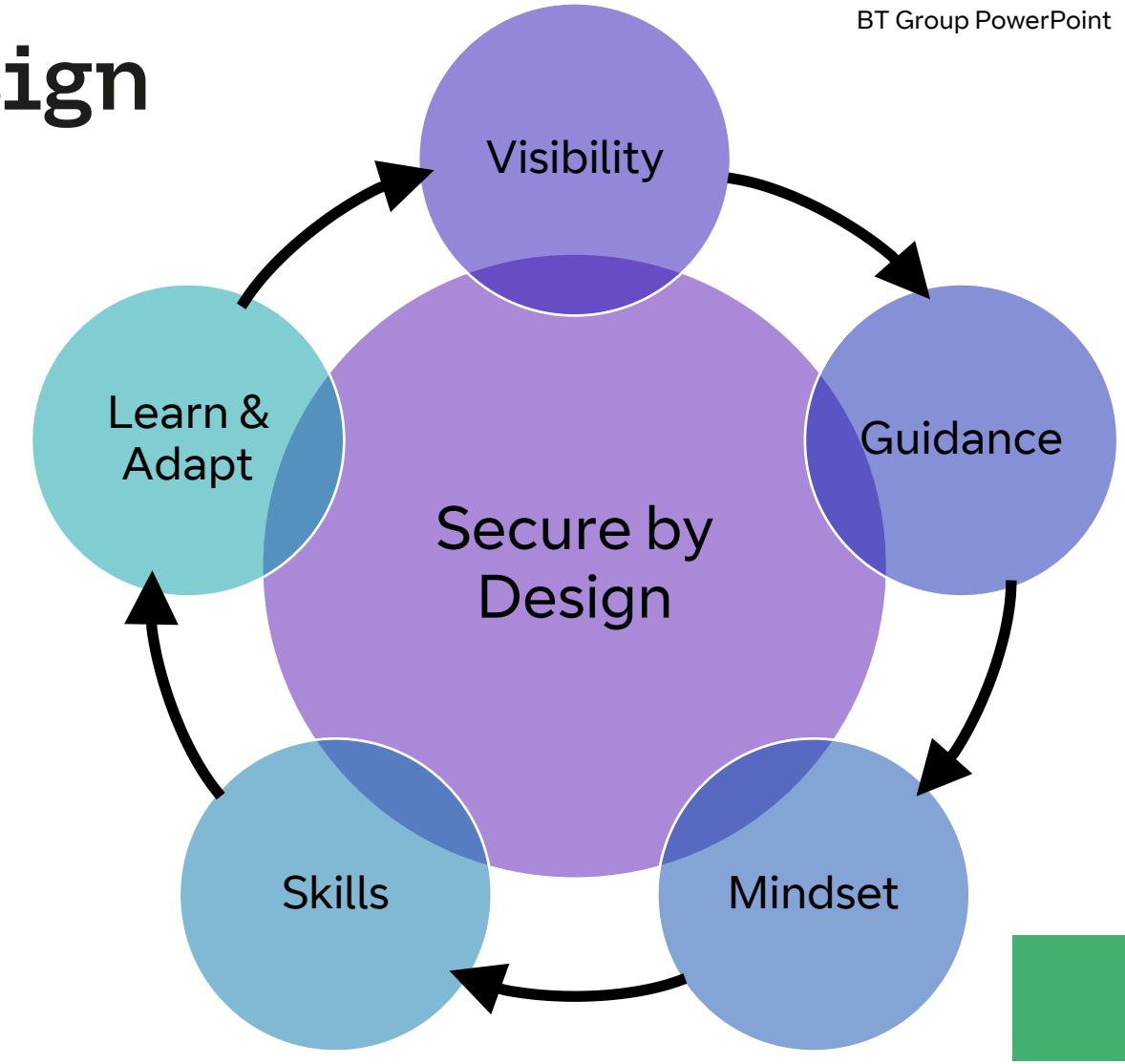
- Giving our service a brand name
- One tool to rule them all
- Too much demand, no plan
- Great at being reactive
- No time to slow down and think
- Approach didn’t scale

What happens in Security…

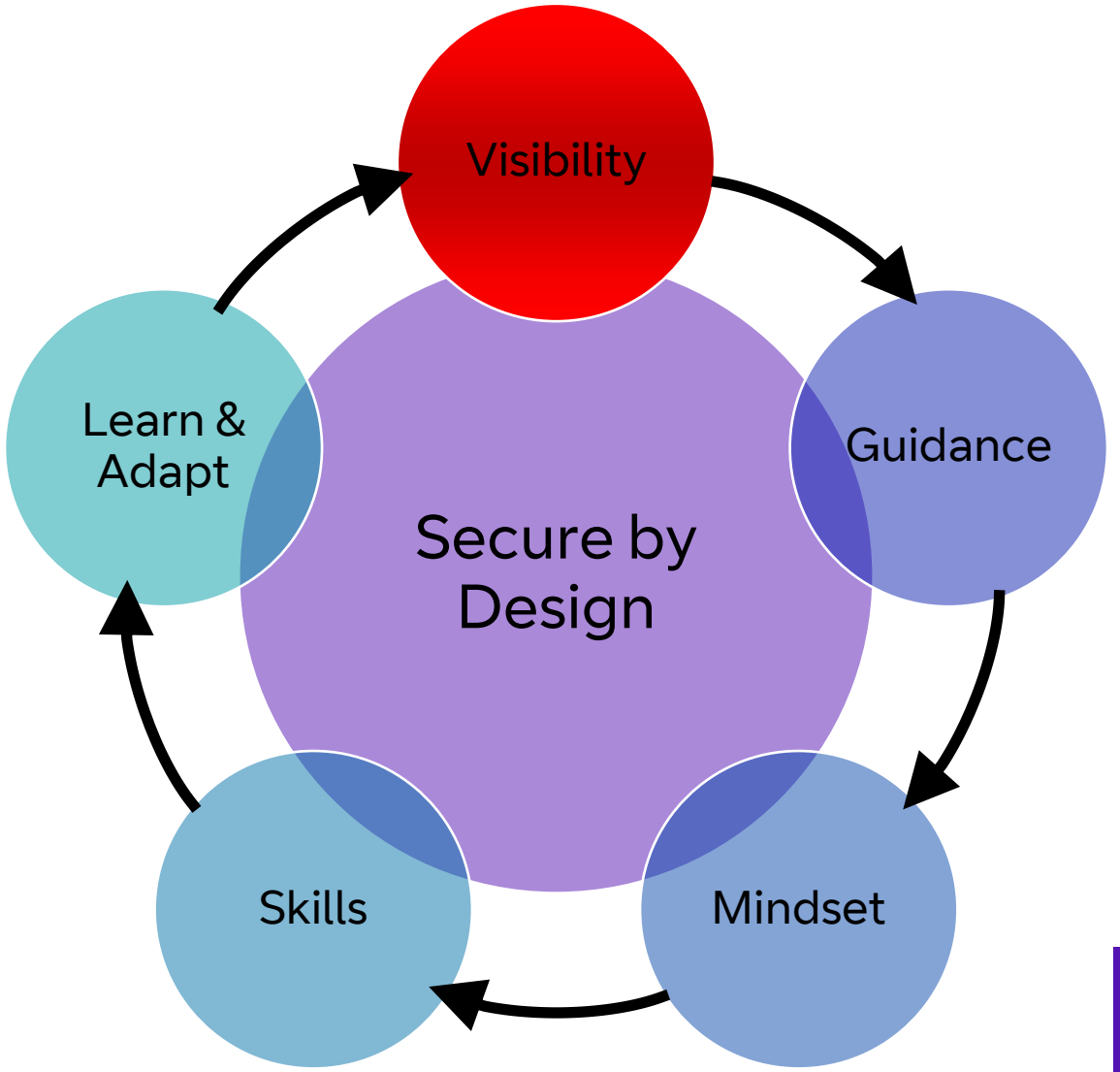


Consistent Secure by Design

- Get visibility of the landscape
- Consistently guide everything
- Lead with an objective mindset
- Get the right skills in the right places
- Fail, learn and adapt



Get visibility of the landscape



Get visibility of the landscape

The importance of situational awareness

The rule of fives

- Who, Why, What, Where & When applied to People, Process and Technology lenses
- Ask why five times (Root cause analysis)
- Leave no stone unturned

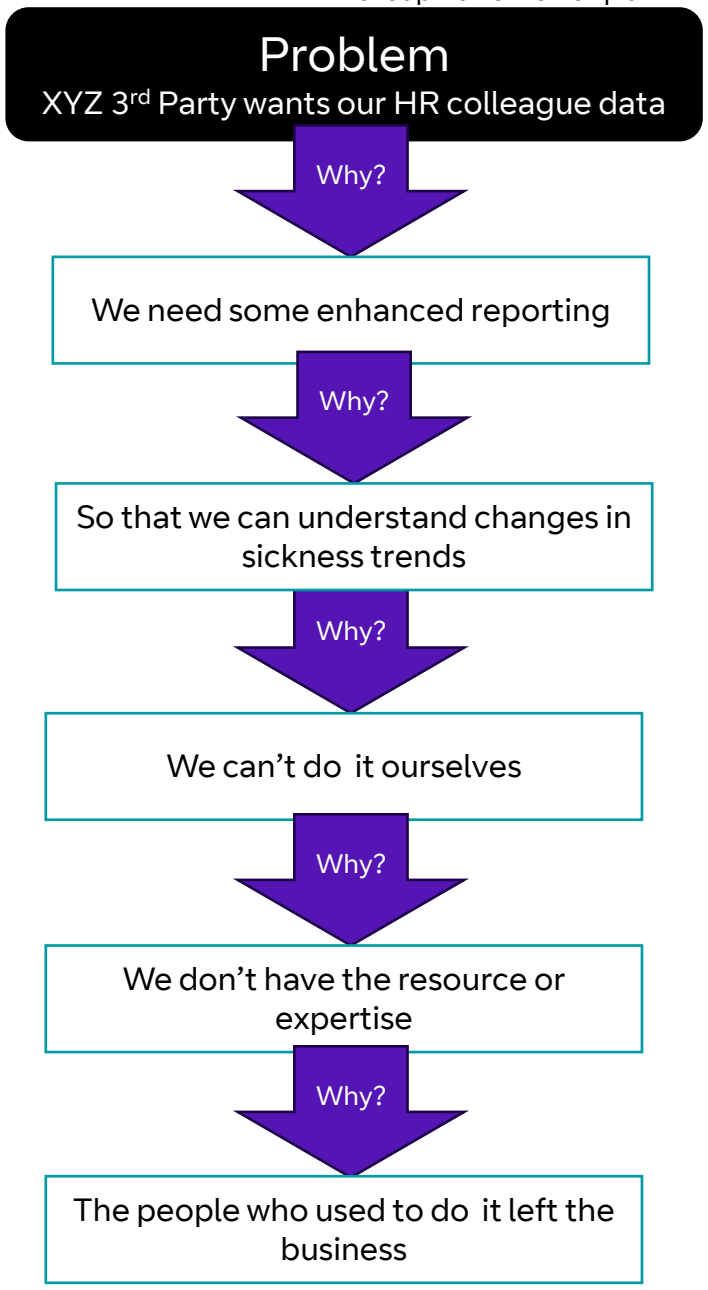
The 7 golden impact zones

- Supplier (3rd Party), data classification, data processing, development, infrastructure, integration, regulatory
- Triage against a high, medium, low impact
- Re-triage if understanding changes

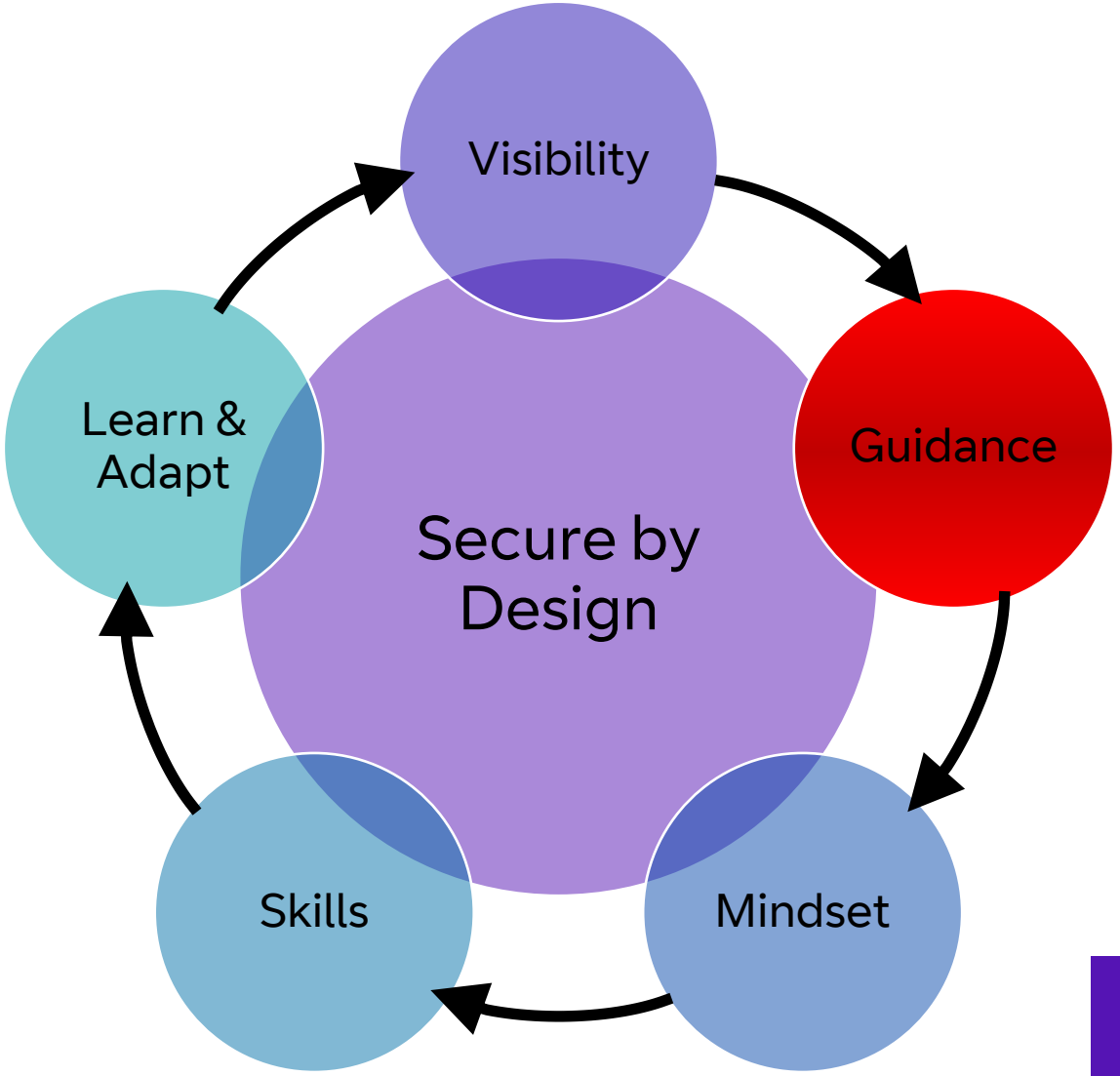
Threat-led & Risk-based

- What is the threat to your assets?
- What is the worst-case scenario?
- What are your red lines?
- Who will take responsibility for risk?

"The original idea is only 2% of the journey" – Sir James Dyson

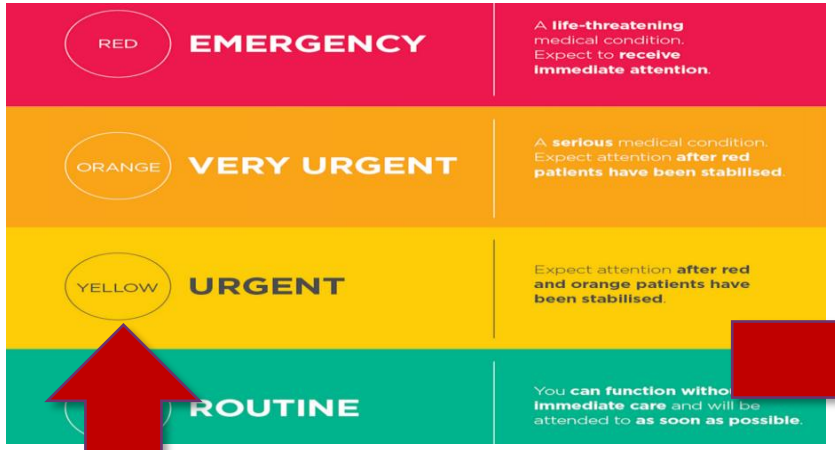


Consistently guide everything



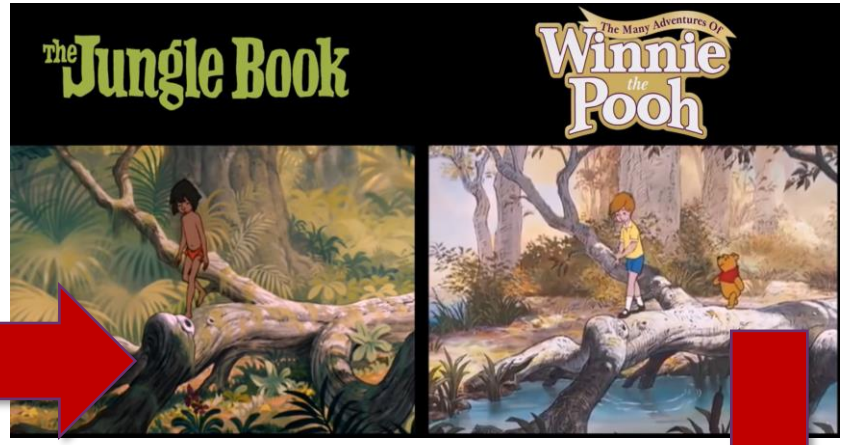
Guiding Secure by Design

A self-healing, self-learning approach



Triage everything!

Threat Assess



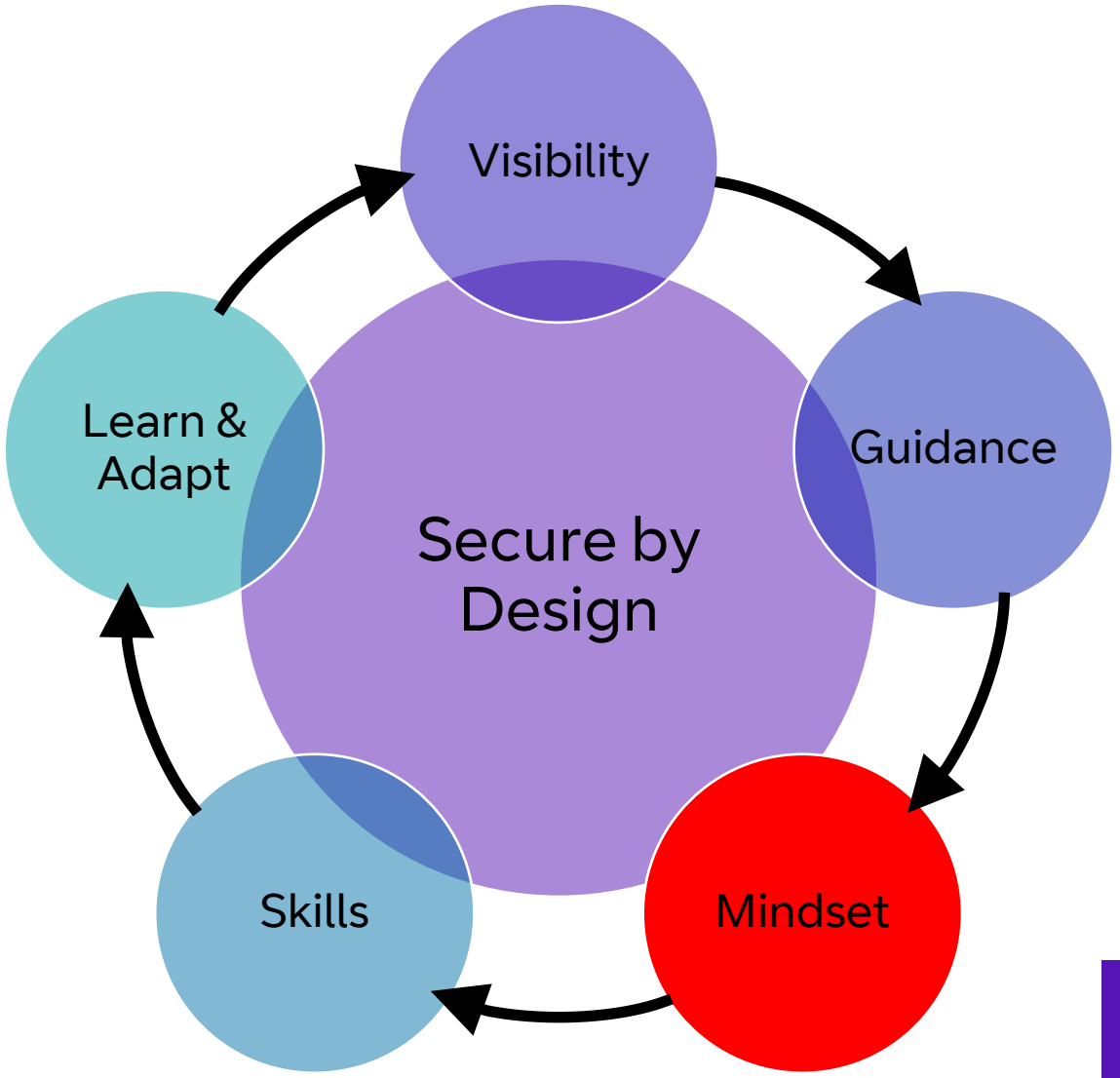
Apply Design Patterns

Uplift Guidance

Risk Assess

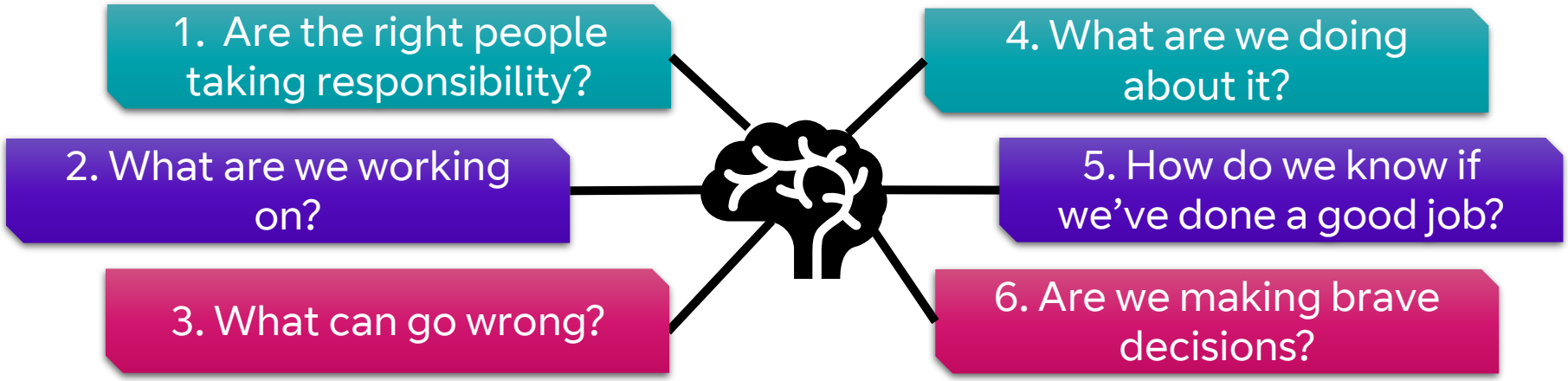
Manage exceptions

Create an objective mindset



Lead with an objective mindset

Enable critical thinking and create accountability



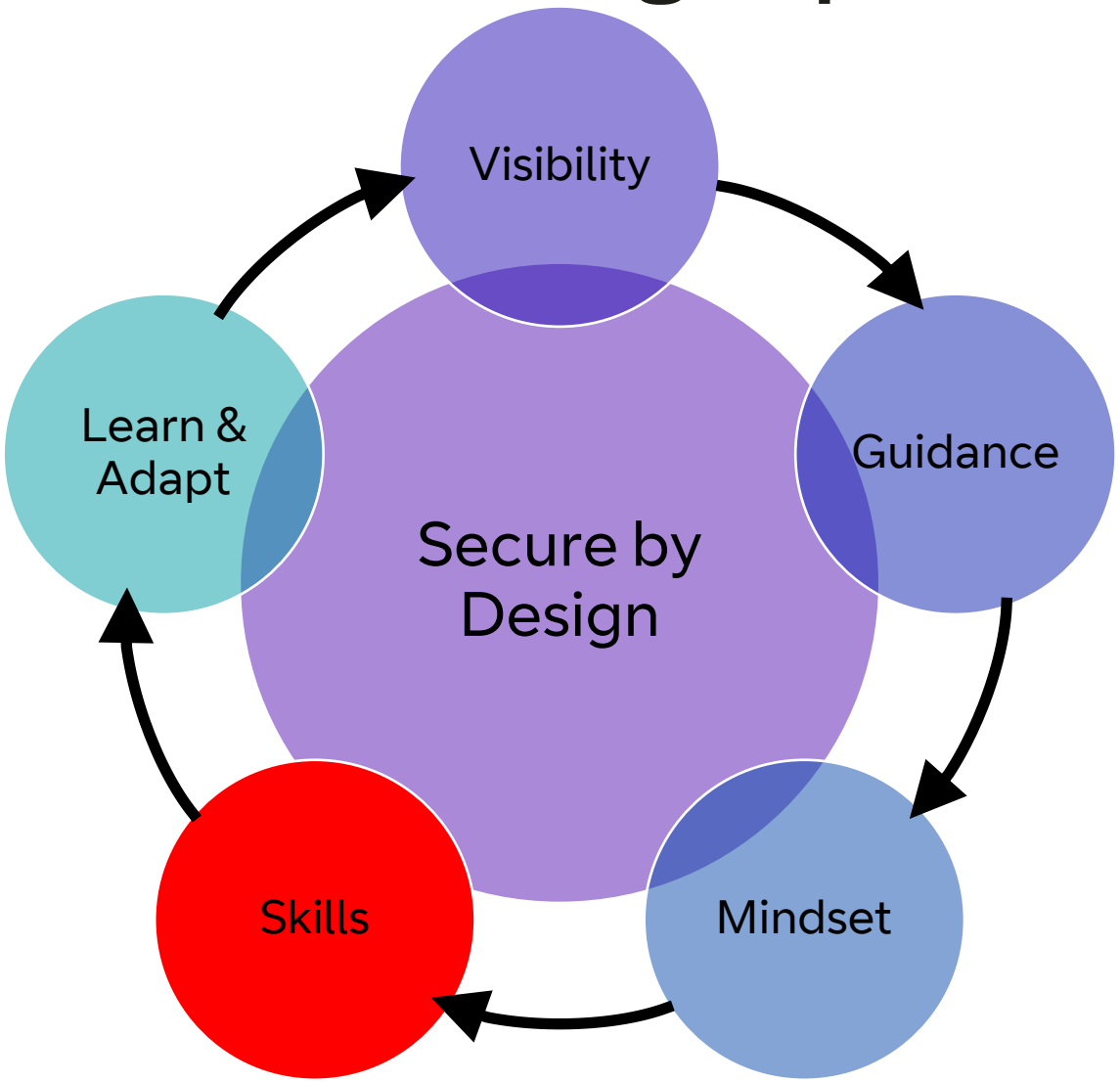
When the stress of "just get it done" takes over, perception narrows, and it takes a disciplined mindset to prevent poor decisions being made.

1. Do we know who needs to make decisions when needed?
2. The context of the work: Who, why, what, where and when?
3. The threat scenarios that keep our eyes open.
4. Are we able to mitigate our threats?
5. Can we evidence that we have good controls?
6. Can we make balanced risk decisions on what's left?

A mindset for everyone in an organisation who has an impact on overall security

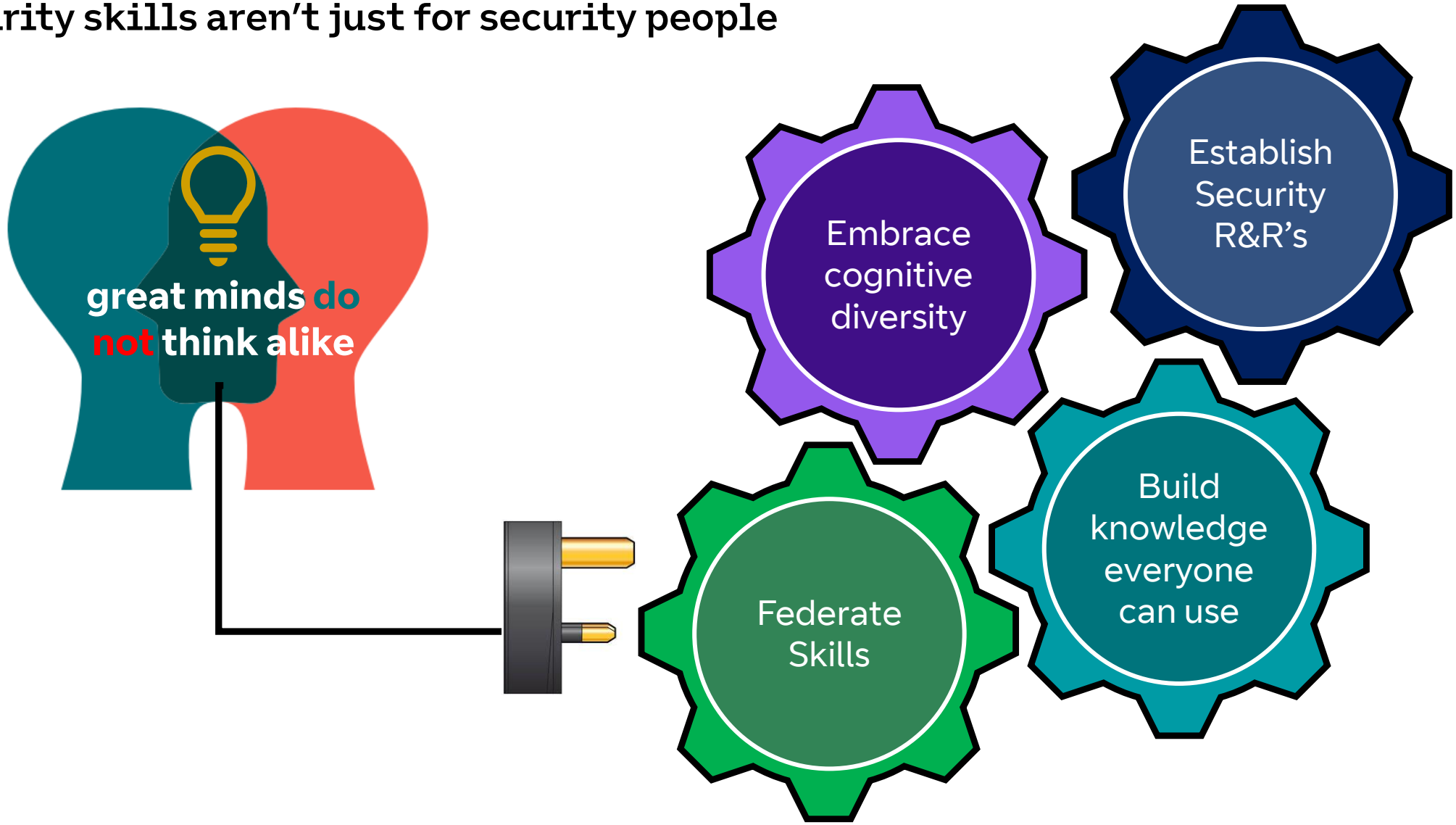
We are hardwired to believe the world is simpler than it really is.

Get the right skills in the right places



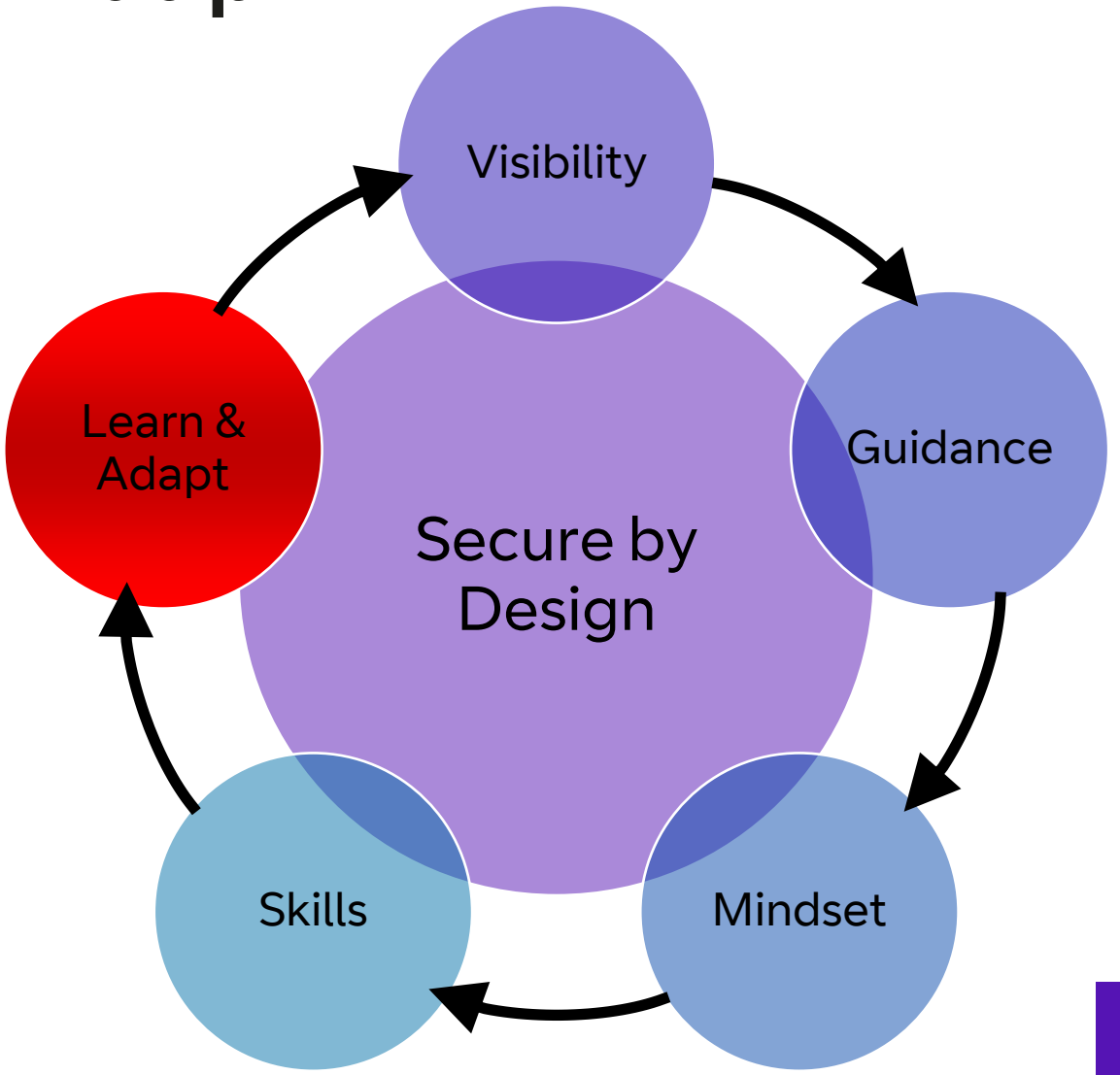
Get the right skills in the right places

Security skills aren't just for security people



The primary goal of security professionals is to make everyone else better at security

Fail, Learn and Adapt



Fail, learn and adapt

Failure + learning = adaptation

Innovate Ways of Working

Marginal gains

Objectivity

Pre and post-mortems

Psychological safety

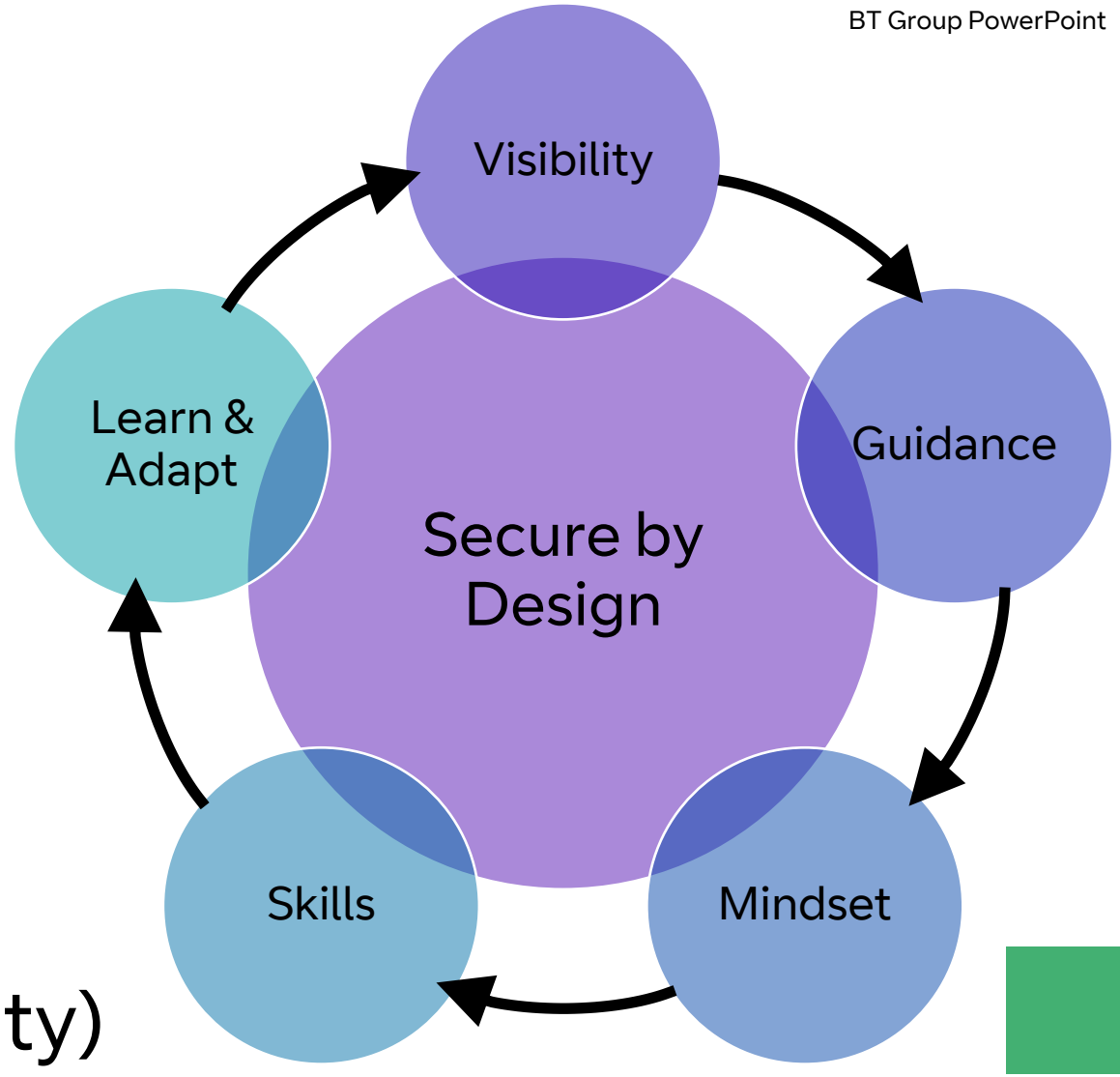
Growth through Failure

Feedback loops

“Failure is simply the opportunity to begin again, this time more intelligently” – Henry Ford

Summary

- Get visibility of the landscape
- Consistently guide everything
- Lead with an objective mindset
- Get the right skills in the right places
- Fail, learn and adapt



Security =
Knowledge + Skill + Luck
(Luck = preparation + opportunity)

Thanks, Questions?