

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



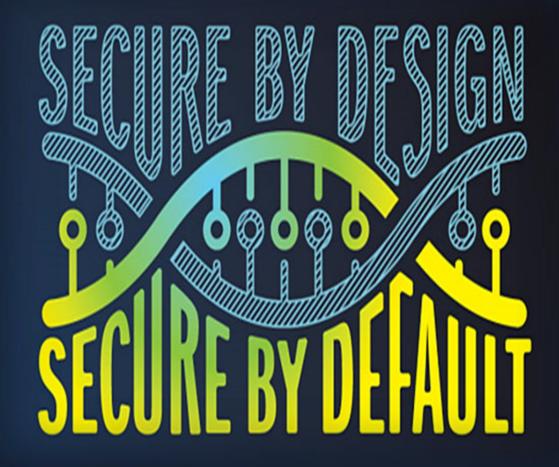
eu.	Medical Expires / / Class/Type Rating Expires / /					0	11.924										mins/deci	mal	and we in a real strength	
AIRCRAFT		Captain	Holder's Operating Capacity	FLIGHT DETAILS		18.0	TRO		2	3	4	5 6 7 8 NIGHT			8	9 10		DAY I GHT		2
Туре	Registration		Contraction of the local division of the loc	From	То	Depart Time	Arriv	Single-Er	DA' ngine (SE)	Multi-Eng	gine (ME)		ngine (SE)	Multi-Eng		Instrument	Any Other Flying	T-O LDG	10000	3
C152	GBUN	PETER SUSADA	P.U.T	EGAL	EGML	11-15	- Im	In Command	Dual or P2	n Command	Dual or P2	In Command	Dual or P2	In Command	Dual or P2	Flight			1	Remarks
PA28	and the second se	PETER SUSRION	Alter and the second	Ehme	1 Cane		11.50		0.6									313	1	CURRENCY CHECK.
PA28	and the second se	DEAN TAYLOR	TAXABLE DOWNERS	EGMC		11.30	1215	-	0.75						-			SIS		PA28 CHECH OCT.
and the second se				2	EGMC	12.05	13.25	1.3										111		LOCAL FLIGHT
PAZZ		DEAN THILOT	Children (1978) - Land (1979) - Children (1979)	EGMC	EGMC	09.00	09.45	0.75										515	1	CIRCUITS
PAZE	GBOTF	DEAN TATLON	PIC	EGMC	ELSU	10.20	and a strength	0.15	and the second s									11		DUXFORD LAND AWAY
PA28	GBSTF	DEAN THTLON	PIC	EGMC	EGSU	12.45	-	0.75	The second s			Sec. 1			1			111	1	RETURN TO SOUTHENS
PA28	GDOTE	RETER SITSREPA	P.U.T	EGAK	EGRE	10.20	11.40		1.0			-						313		Flight satis factory AC
CISZ	GBaco	DEAN TATION	P.1.C	EGMC	EGMO	11.35	12-20	0.75	Sector Control of Cont									111	1	Le00 -
PA28	GATPN	DEAN TATION	P.I.C	EGMD	EGMC	1600	16-45	0.75										111	1	SOUTHEND
CISZ	GBSZO	Dean TAYLON	P.1.C	EGMC	EGME	09.50	10.40	0-85										111	1	LOCAL NOTICE EASI
		Dean Taylor		EGMC	ESSC	09.25	6-0	0-7	007			N			1			(1)		CAMBRIDGE
		Per Taylor		EGSC	EGMC	10.40	1130	0-85	\$									(11		SOUTH END
CK2	GRS20	eter Shorter	PUT	San The State of State	EGAL	10-07	10-42		0.4									313		90 DAY CHECK
CIS2	(102	0 Gibrier	0.1	EGMC	and the second sec	10.45	11.10.	04	-									313		SOLO CIRCUTTS
CISC	10320 1	Den Taylor	P.I.C	EGAL	EGAL	FI	LYING TIM	Start Di	1.00									hrs		I certify that the entries in this log are true
							carl	19710751	-			-		1	The states	1		1 2 12 2		

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"

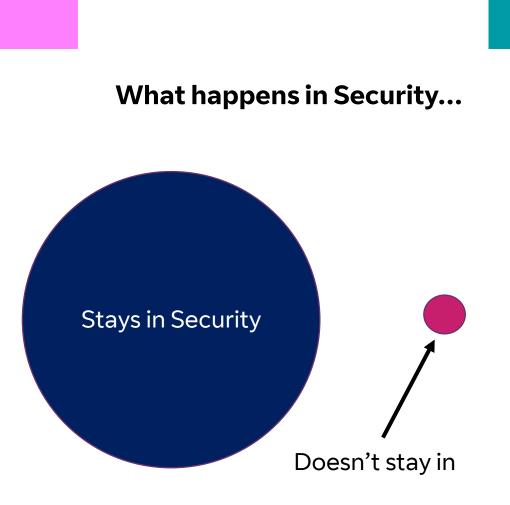
How it began...

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



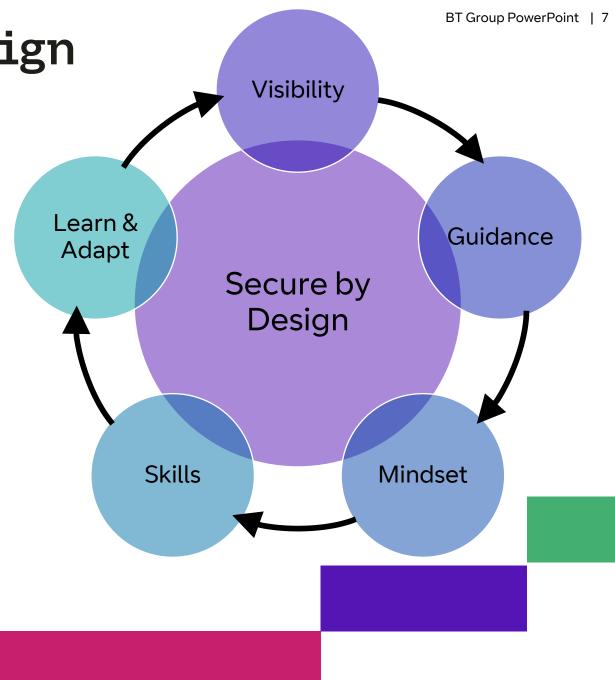
Early Mistakes

- 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

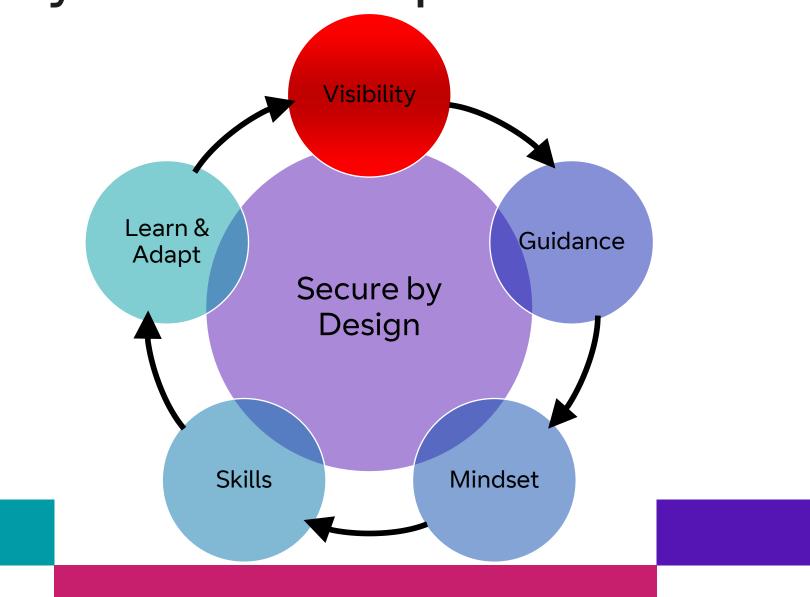


Consistent Secure by Design

- 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 7 golden impact zones

The rule of

fives

Supplier (3rd Party), data classification, data processing, development, infrastructure, integration, regulatory
Triage against a high, medium, low impact

• Who, Why, What, Where & When applied to People,

Re-triage if understanding changes

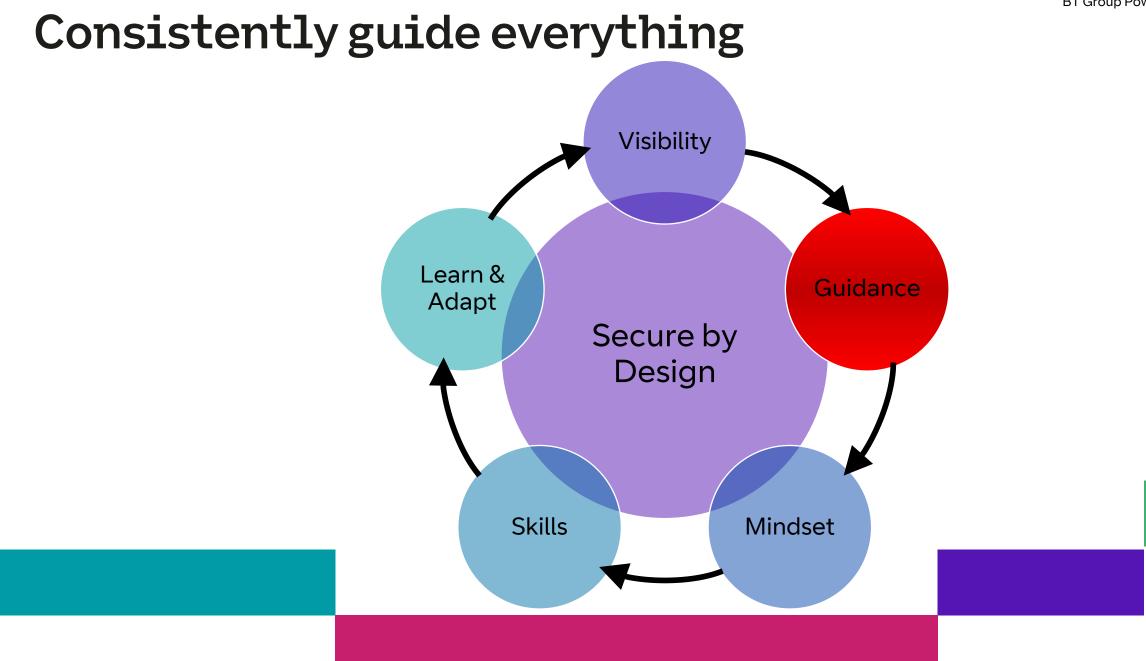
Process and Technology lenses

Leave no stone unturned

• Ask why five times (Root cause analysis)

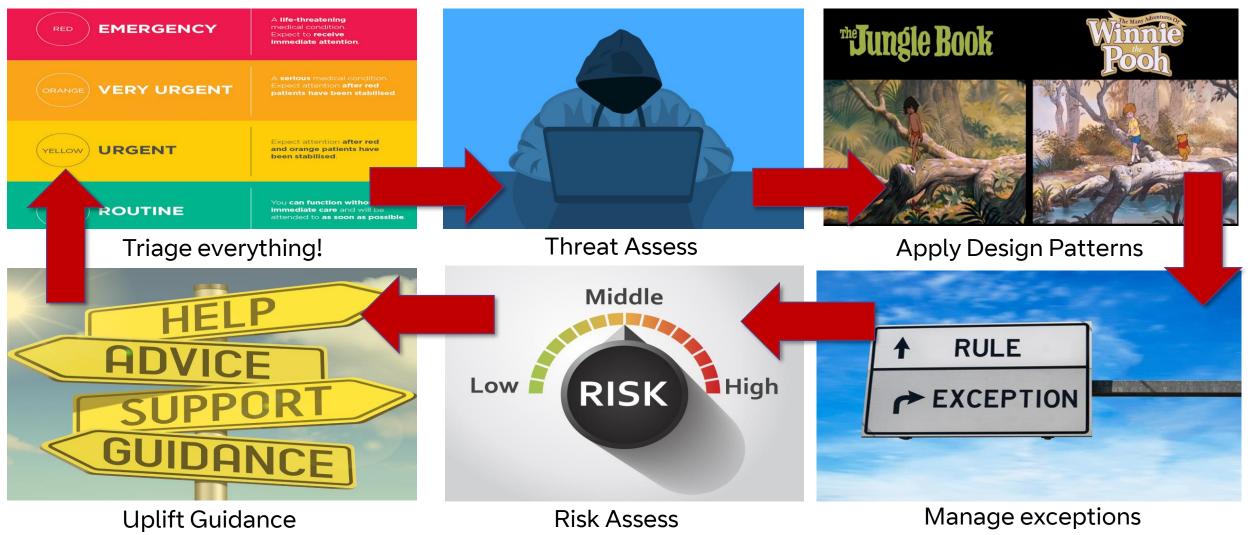
Threat-led & Risk-based

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

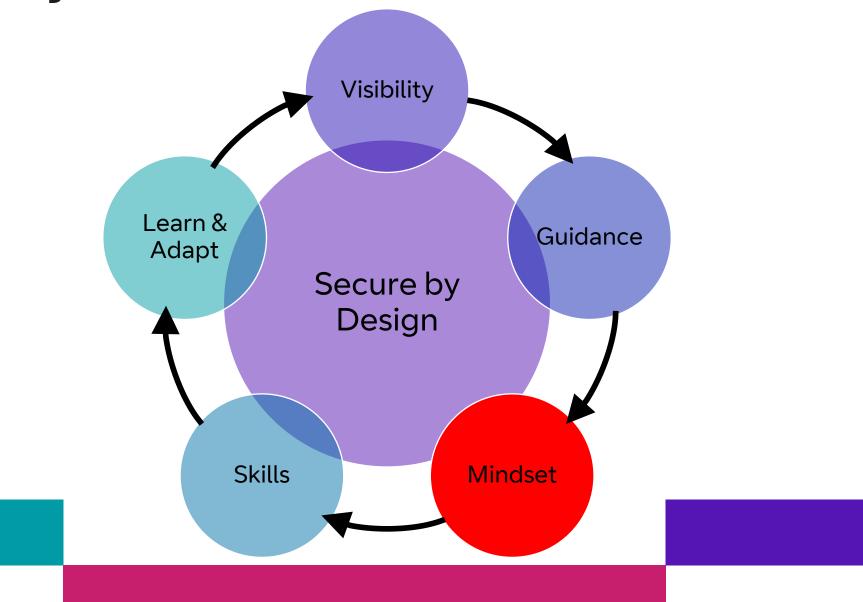


Guiding Secure by Design

A self-healing, self-learning approach

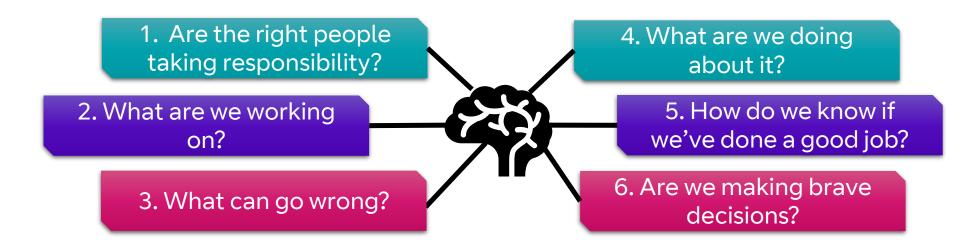


Create an objective mindset



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.



Do we know who needs to make decisions when needed? The context of the work: Who, why, what, where and when? The threat scenarios that keep our eyes open.

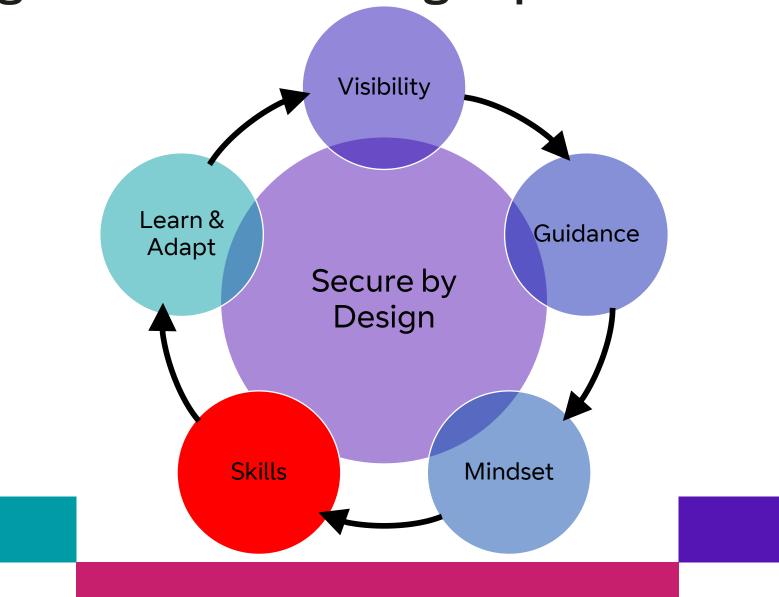


Are we able to mitigate our threats? Can we evidence that we have good controls? Can we make balanced risk decisions on what's left?

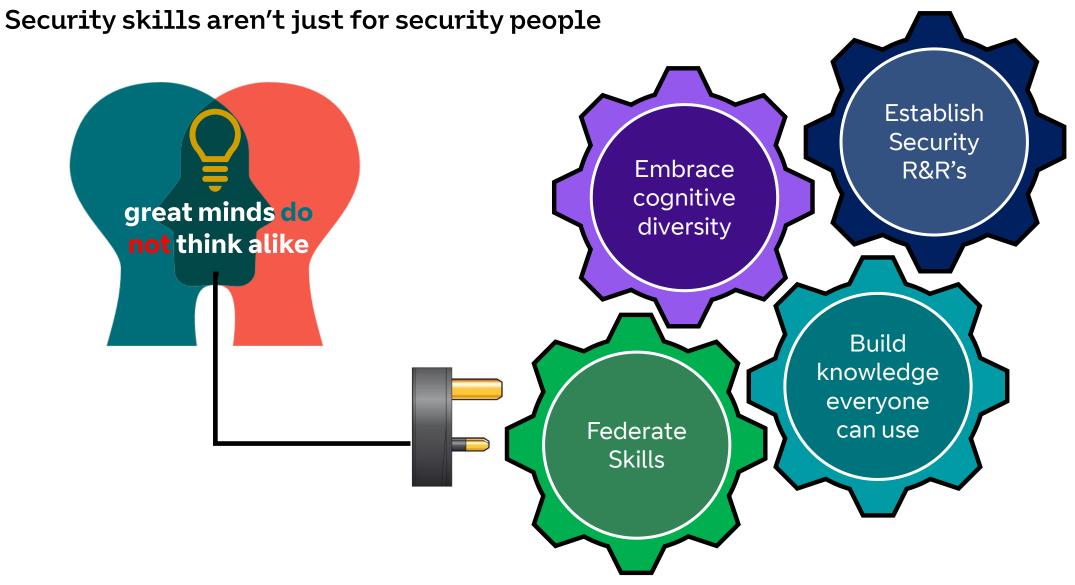
A mindset for everyone in an organisation who has an impact on overall security

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

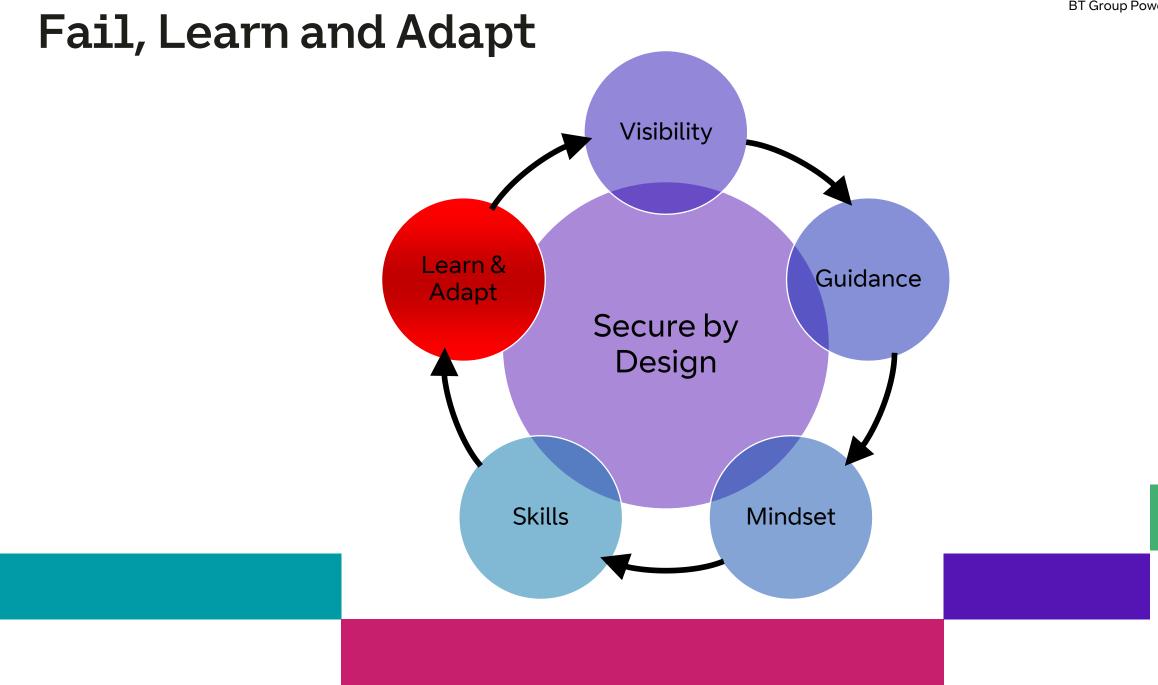
Get the right skills in the right places



Get the right skills in the right places

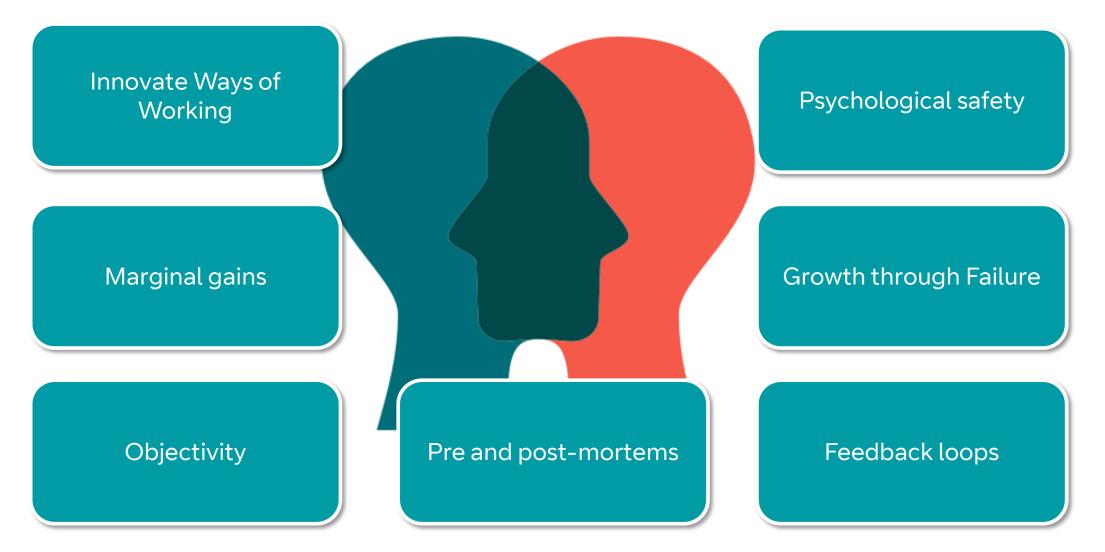


The primary goal of security professionals is to make everyone else better at security



Fail, learn and adapt

Failure + learning = adaptation

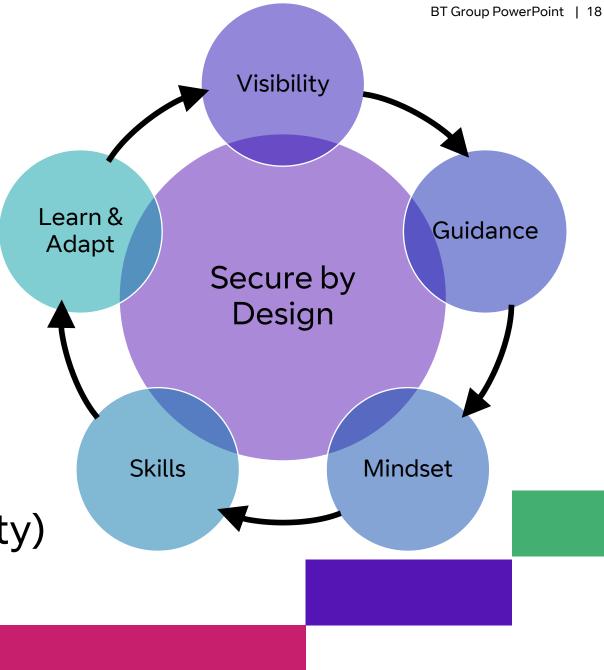


"Failure is simply the opportunity to begin again, this time more intelligently" – Henry Ford

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?



"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"