

# Security Culture Transformation

Identify and address your organisation's human-centric risks



**A healthy security culture is the foundation of sustainable organisational resilience. Efforts to improve security culture often fail to produce the desired effect because they focus on security awareness, which is only one of many underlying causes of poor security attitudes and behaviours.**

KPMG's approach to identifying and addressing human-centric risks is holistic, data-driven, and focused on moving organisations towards a culture of continuous improvement. We assess your current human-centric risks and develop a prioritised program of targeted interventions that address your unique critical risks.

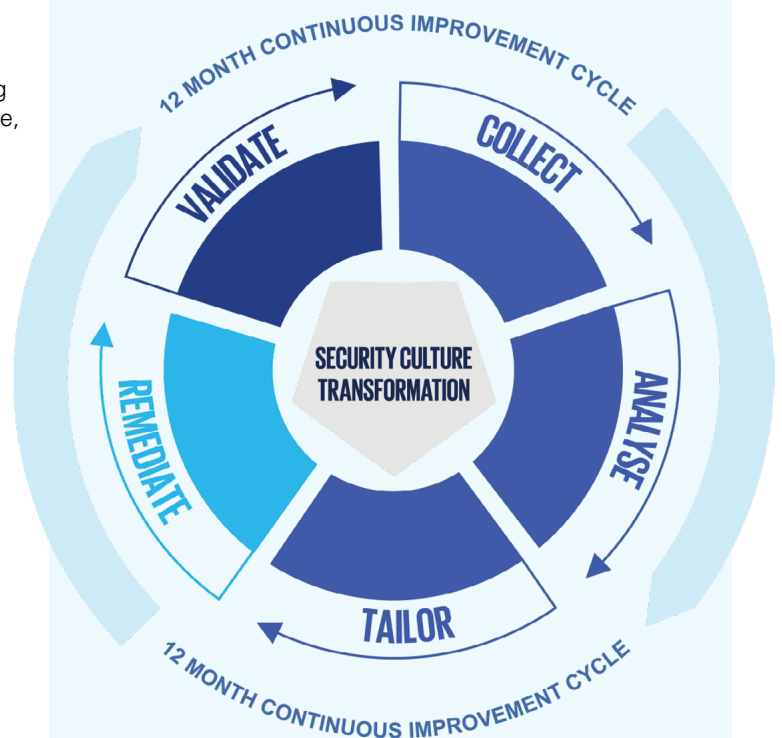
# 82%

**of breaches involve the Human Element, including Social Engineering Attacks, Errors and Misuse.**

Data Breach Investigations Report, Verizon 2022

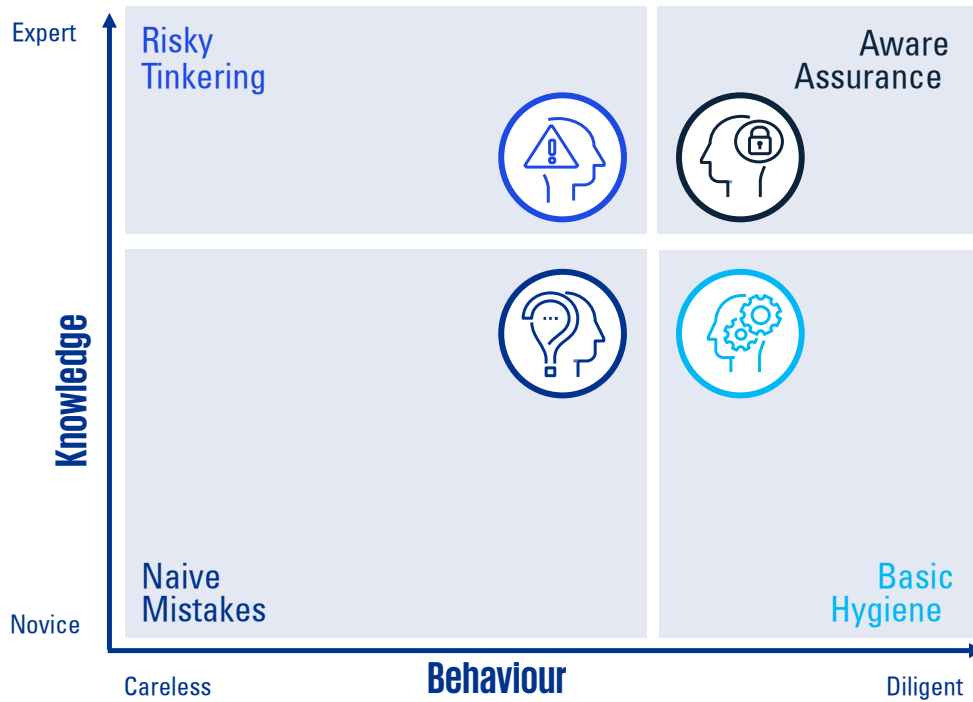
## Continuous Improvement for Organisational Security Culture

- 1 Collect**  
Assess your Security Operating model, including a diagnostic to measure staff security knowledge, attitudes and behaviours.
- 2 Analyse**  
A comprehensive report of your Security Culture, diagnosed using KPMG's leading methodology and toolset.
- 3 Tailor**  
A tailored business case with prioritised intervention strategies to uplift your organisational security culture.
- 4 Remediate**  
A focused work program of change interventions to reduce your key human-centric risks.
- 5 Validate**  
A pulse check to measure the effectiveness of change interventions in addressing your key human-centric risks.



# Security Culture Personas

KPMG measures security knowledge, attitudes and behaviours across an organisation's workforce. We reveal human-centric risks that undermine your organisation's security posture.



Once understood, we deliver tailored intervention strategies unique to your cultural strengths and weaknesses. These can be measured over time, demonstrating increased organisational resilience and security culture maturity.

## Contact us



**Drew Baker**  
**Partner**  
People & Change  
KPMG Australia  
drewbaker@kpmg.com.au



**Greg Miller**  
**Partner**  
Cyber & Critical Infrastructure  
KPMG Australia  
gmiller3@kpmg.com.au

**KPMG.com.au**

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2023 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation. March 2023. 1025047301CYBER.