Cyber Security Culture

Identify and reduce your organisation's human-centric risks

People, not technology are the biggest risk when it comes to cyber security and data breaches.

KPMG's diagnostic approach to identifying and reducing human-centric risks is holistic, data-driven, and focused on moving organisations towards a culture of continuous improvement. We provide a measurable and repeatable method that includes targeted interventions to minimise your organisation's exposure to cyber security threats.

"74%

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

Data Breach Investigations Report, Verizon 2023

Do you know the cyber security risk behaviours of your workforce?

We identify human-centric risks of your organisation by measuring the knowledge, attitudes and behaviours of your workforce. This data-driven approach identifies positive and negative cultural traits as well as key risks impacting your organisation's security posture.

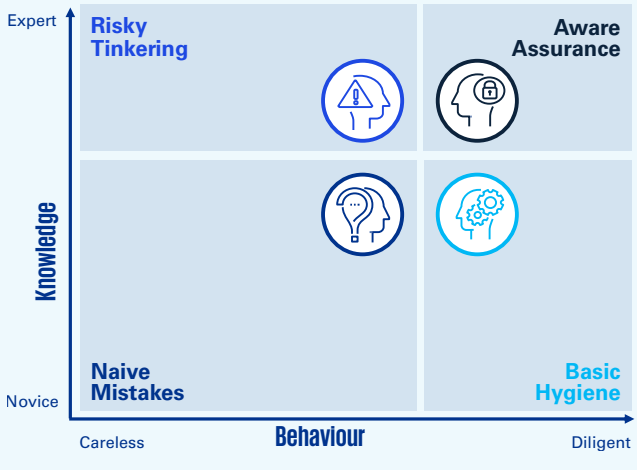
Knowledge
What people **know** about security

Attitudes
What people **think** about security

Behaviours
What people **do** about security

Know the drivers to mitigate risk

KPMG measures security knowledge, attitudes and behaviours across an organisation's workforce to reveal potential drivers of the identified human-centric risks. This is visualised through segmentation of workforce by risk persona type.



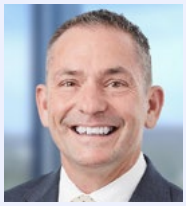
By bringing to life the risky behaviours and cultural traits undermining your organisation's security posture, we can target and tailor interventions to where they are needed most.

How KPMG can help you

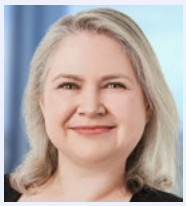
Once your human-centric risks are understood, we develop **tailored intervention strategies to address each risk and its driver**. Over time we can help you remeasure your cyber security culture maturity to gauge the effectiveness of each intervention strategy at reducing your risk.

Our data-driven approach is designed to give you the evidence base and the business case to embed a more resilient workforce capable of combating current and emerging cyber and security threats.

Contact us



Drew Baker
Partner
Consulting
KPMG Australia
E: drewbaker@kpmg.com.au
M: 0414 477 417



Alex O'Rourke
Director
Cyber HRM and Policy
KPMG Australia
E: aorourke1@kpmg.com.au
P: +61 2 6218 6578

We work with you over a 10-12 week period to analyse your current human-centric cyber and security risks and risk drivers. On completion, we provide you with a data-driven diagnostic assessment report that details your organisaton's current state cyber security culture, and an action plan to manage and reduce your human-centric cyber and security risks.

In addition to helping your organisation identify, understand and mitigate human-centric security risks, our approach can also help you to improve governance and accountability by providing:

Tailored human risk mitigations

Implement tailored intervention strategies to improve the maturity of your organisation's cyber security culture over time.

Measurable enterprise security culture

Understand the current maturity level of your organisation's cyber security culture, with the ability to zoom in by business lines.

Organisational benchmarking

Benchmark against similar organisations and run annual pulses to see change over time.

Data-driven return on investment

Provides a data-driven ROI mechanism for human risk reduction interventions like security training.

KPMG.com.au

 April 2024. 1325455599CON.