



KPMG Cyber Risk Insights

Advance cyber risk
management and
decision-making



What it is:

A solution to quantify cyber exposure and prioritise investment decisions

CISO & Security Leaders



Boards and Executive Management



Risk Management Team



Why it matters

Traditional maturity assessments and risk registers describe control posture but do not quantify financial consequences or show which investments reduce exposure most effectively. As boards seek clearer trade-offs, CRI connects threat scenarios, capability effectiveness and potential losses to provide decision-relevant insights on risk appetite, investment priorities and expected risk reduction.

**Quantify cyber exposure and
prioritise investment decisions**

What it does: Turn cyber risk into financial and business impact for better decision-making

Identify potential control gaps

Quantify cyber risks and associated financial impacts.

Prioritise cyber investments

Maximise risk reduction from available resources.

Strengthen executive reporting

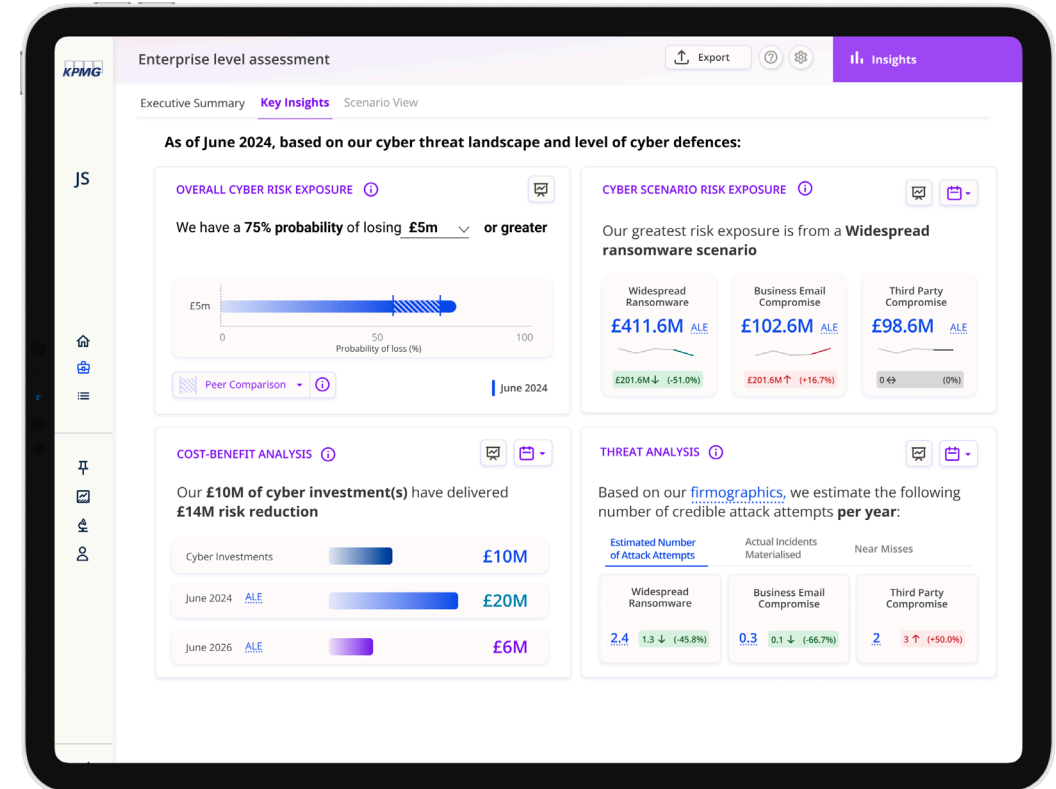
Communicate cyber risk and gain stakeholder buy-in.

Benchmark their cyber posture

Assess performance against industry peers.

Benefits

- Clearer visibility of cyber risk and risk appetite
- Defensible investment and remediation priorities
- Stronger board-level decision support



How it works: Connect organisational data to risk decisions

Input

The organisation provides scenario, threat, control effectiveness and context-specific loss information.

Action

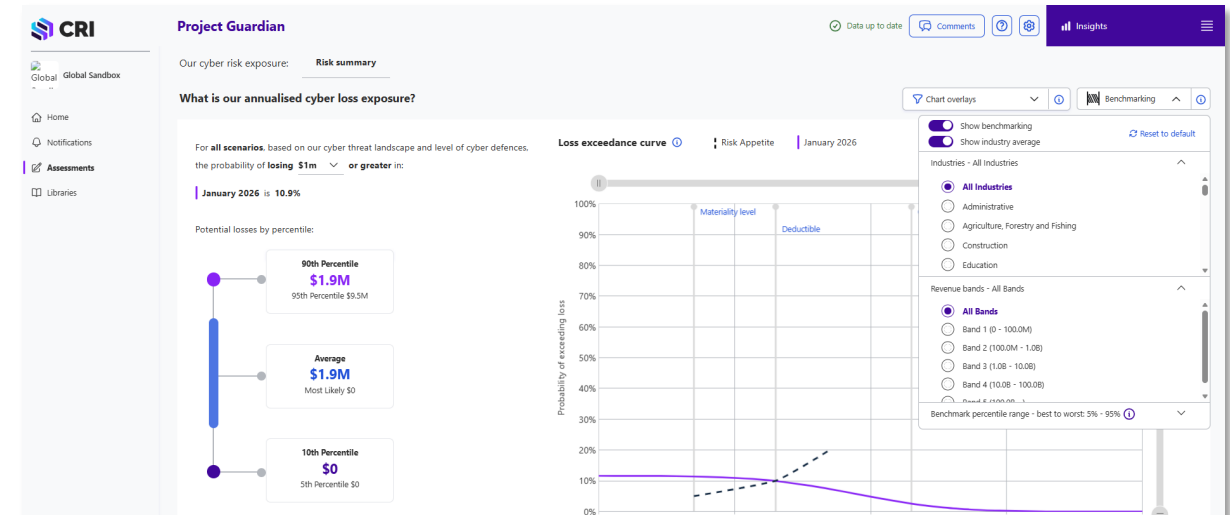
CRI applies scenario likelihood, capability, financial impact and cost-benefit modelling.

Output

Leaders receive quantified exposure, capability gaps, scenario priorities and investment analysis.

Impact

Decision-makers can prioritise actions and investments that provide the greatest risk reduction relative to cost.



Quantify your cyber exposure with confidence

Discover how scenario-driven analysis can turn cyber risk data into clearer investment, resilience and risk appetite decisions.

Consider a discussion if your organisation is:

- Prioritising cyber investments under budget constraints
- Assessing exposure against organisational risk appetite
- Evaluating third-party, resilience or transformation risks

Explore your priority cyber risk scenarios with us.



Sanjai Sivasankar

**Associate Director, Cyber,
KPMG in Singapore**

sanjaisivasankar@kpmg.com.sg

CRI scenario-driven approach to assess your threat profile

CRI comes with twelve scenarios out of the box

We bring a suite of pre-defined scenarios that provide comprehensive coverage of cyber risks and exposures. Additional scenarios can be tailored to your environment and requirements.



Accidental data disclosure



Accidental digital services compromise



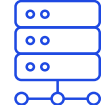
Business email compromise



Cloud environment compromise



Distributed Denial of service



External major data breach



Insider data breach



Insider major data breach



Insider software compromise



Third party compromise



Web framework compromise



Widespread ransomware



Likelihood logic

- Aligned to Lockheed Martin Cyber Kill Chain and ISF Cyber Attack Path
- Inspired by and incorporating MITRE ATT&CK framework techniques in a more practical fashion
- Proofed by modelling teams



Cyber threat scenarios

- Produced using real-world, historical attacks
- Validated by incident response and penetration-testing teams
- Refined with input from world-leading insurers, banks and manufacturers



Loss model provenance

- Based upon Douglas Hubbard and FAIR's approach
- Reviewed by actuarial modelling teams

The model is reviewed and updated quarterly.



KPMG Services Pte. Ltd.

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

General disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. 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.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public