

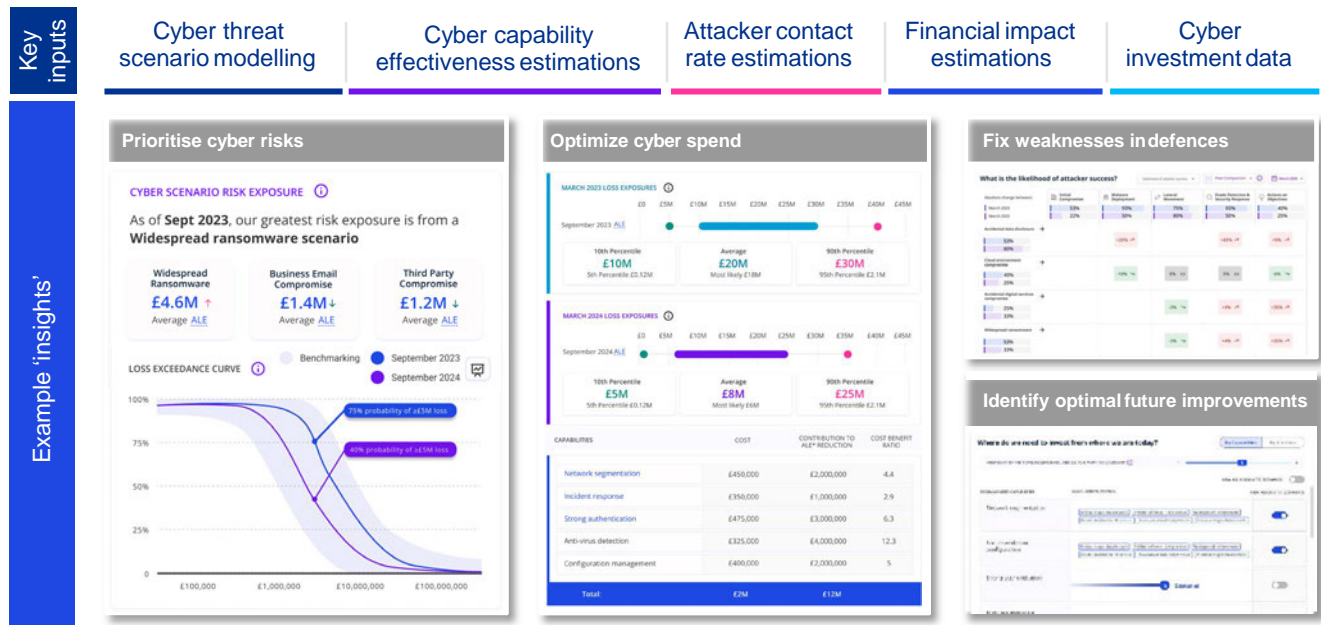


# Cyber risk insights

A market leading product to help you make better cyber risk decisions

## What is KPMG Cyber Risk Insights (CRI)?

CRI is a licensable SaaS product, which takes a scenario-driven approach to more accurately assess the likelihood and impact of cyberattacks. It uses powerful and intuitive dashboarding to show insights with a strong user interface.



## Why use KPMG CRI?

CRI gives you a comprehensive view of the potential financial losses in the event of a cyberattack, as well as the best 'bang for buck' investments to help mitigate those attacks. This allows you to make defensible and data-driven decisions and can help you prioritize your remediation efforts. The typical questions CRI helps answer are below.

Prioritize cyber risks	Regulator(s) Board CEO CFO COO CIO CRO CISO Business	What is our true risk exposure to cyber attack (likelihood in a year and potential financial impact)? Is it within our risk appetite? What cyber risks should we prioritise?
Optimize cyber spend	Board CEO CFO COO CIO CISO Business	What cyber investments would deliver best bang-for-buck risk reduction? If year, is we invest XM in cyber next this too much or too little?
Improve communication	Board CEO COO CIO CRO CISO Business	I know cyber is a complex risk with many interdependencies – how can we simply explain our overall exposure in order to make effective well-informed decisions?
Comply with regulation	Regulator(s) Board CEO CRO CISO	How can I determine the potential 'material' impact of a cyber attack on my business? How can I communicate cyber risk to the Board to meet new cyber reporting requirements?

# Some key benefits

CRI equips you with the tools to:



## Make the case to the board

CRI's logical and transparent approach helps you to communicate cyber risk to senior stakeholders, demonstrate the business benefits of cyber capabilities, and make compelling investment cases.



## Carry out systematic, consistent, data-driven assessments

CRI makes the adoption of quantitative techniques quick and simple. It improves the objectivity of risk assessments by producing consistent, data-driven results.



## Quantify likelihood and impact

Access to our tried and tested models, which quantify the likelihood of cyber risk scenarios occurring, the possibility of attackers succeeding across the layers of defence and potential financial losses.



## Target spend to reduce exposure

Graphical risk scenario models allow you to see where your cyber capabilities contribute to risk reduction across the layers of defence and which areas would benefit most from investment.



**Help optimize investments** Determining the optimal investment portfolio of cyber capabilities to help achieve a great return on investment in risk reduction.



## Test investments

Estimate the payback period for an investment or investment portfolio, based on a cost-benefit analysis of spend compared to the expected reduction in cyber losses.

Contact us to discuss your organization's needs or to arrange a demo of our Cyber Risk Insights (CRI) product.

## Contact us

### Paul Sammut

KPMG in Canada  
Cyber Risk Insights Lead  
paul.sammut@kpmg.ca

### Adil Palsetia

KPMG in Canada  
Cyber Risk Insights Lead  
apalsetia@kpmg.ca

### Jason Flannery

KPMG in Canada  
Cyber Risk Insights Subject Matter Specialist  
jasonflannery@kpmg.ca

# How has CRI helped our clients?

CRI has helped organisations across a wide range of industries.

## Board confidence and risk reduction

Retail

A historic commitment to align with ISO27001 resulted in the organization trying to fix everything, well beyond their capacity for change. CRI enabled:

- ✓ The de-scoping of 20% of ISO27001 controls based on CRI's threat modelling and What-If simulation capability.
- ✓ C\$850k+ cost saving, whilst also enabling defensible prioritization decisions.
- ✓ Ongoing measurement of cyber risk exposure over time.

## Prioritization of a cyber roadmap

Insurance

A CISO was receiving Board-level challenge about the benefit of the cyber investment program and was asked to reduce spend. CRI enabled:

- ✓ Identification of the priority controls for investment based on robust cost-benefit analysis.
- ✓ Demonstrable year-on-year reduction in cyber risk exposure tied to benefits tracking of change initiatives.
- ✓ Granular assessments of individual business units after the group-wide assessment.

## Managing exposure across a portfolio

Private equity

Cyber risk assessments and remediation plans were required across 20+ portfolio companies. CRI enabled:

- ✓ Each portfolio company to understand their cyber risk exposure, in financial terms.
- ✓ Each portfolio company to prioritize their cyber investments based on the specific threats to their business.
- ✓ The replacement of their 1-5 maturity assessment methodology, giving leaders better confidence in the security of their portfolio.

# What to expect from a CRI assessment?

A typical CRI assessment includes four phases.

01

Week 1

## Scoping

- Identification of exam questions to be answered.
- Identification of potential data sources within the organization to augment KPMG's data sets.

02

Week 2-3

## Scenario selection

- Identification and attack-tree modeling of priority cyber threat scenarios, accelerated by KPMG's existing scenario model library.

03

Week 3-6

## Estimation and measurement

- Estimate and measure required inputs for KPMG's cyber risk quantification models.

04

Week 4-8

## Analysis and reporting

- Reporting to show outputs that answer exam questions identified in phase one.
- We will take your key stakeholders on the reporting journey with us, ensuring that they have the opportunity to buy-in early to a quantitative reporting approach.