Solution Cyber Risk Insights (CRI) de KPMG

Une solution inégalée sur le marché qui vous aide à prendre de meilleures décisions en matière de cyberrisques

Qu'est-ce que la solution CRI de KPMG?

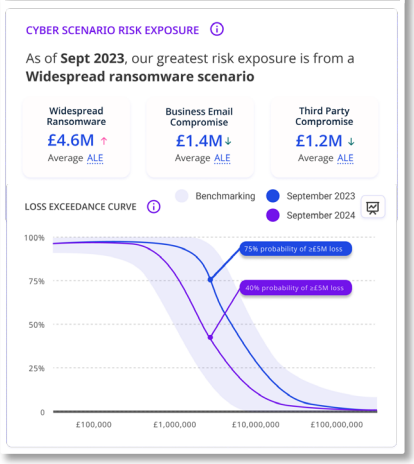
La solution CRI est un produit SaaS (logiciel-service) qui permet, à partir d'une approche fondée sur des scénarios, d'évaluer avec précision la probabilité et l'impact des cyberattaques. Par le biais d'une interface utilisateur optimisée, elle présente des informations utiles tirées de tableaux de bord performants et intuitifs.

Intrants clés

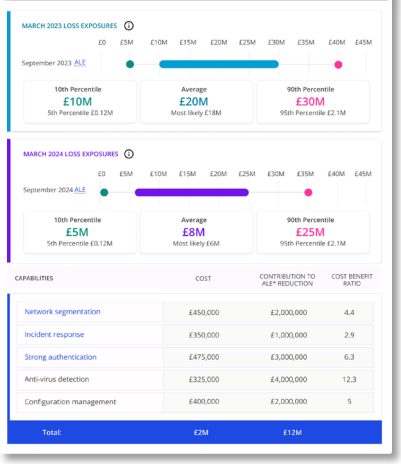
- Scénarios de cybermenaces modélisés
- Estimations de l'efficacité des capacités de réponse
- Estimations de la fréquence des attaques
- Estimations des répercussions financières
- Données sur les investissements en cybersécurité

Exemples d'analyses*

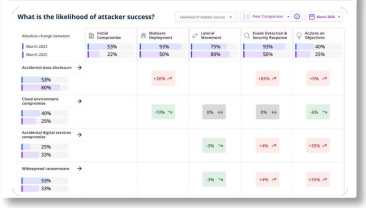
Hiérarchiser les cyberrisques



Optimiser les dépenses en cybersécurité



Corriger les faiblesses des défenses



Définir les améliorations futures

**Cette section présente des images tirées des tableaux de bord de la plateforme ACR, qui ne sont disponibles qu'en anglais*

Pourquoi utiliser la solution CRI de KPMG?

La solution CRI présente une vue d'ensemble des pertes financières potentielles en cas de cyberattaque, ainsi que les investissements les plus rentables pour en atténuer les répercussions. Cela vous permet de prendre des décisions valables fondées sur des données et d'établir l'ordre de priorité des mesures correctives à prendre. Voici des exemples de questions auxquelles la solution CRI peut répondre :

Hiérarchiser les cyberrisques

Org. de régl. | CA | CD | CF | CE | CI | CGR | RSSI | Société

Quelle est notre exposition réelle au risque de cyberattaque (probabilité sur un an et impact financier potentiel)? Ce risque se situe-t-il dans les limites de notre propension au risque? À quoi devrions-nous nous attaquer en premier?

Optimiser les dépenses en cybersécurité

CA | CD | CF | CE | CI | RSSI | Société

Quels investissements seraient les plus efficaces pour réduire les risques? Un investissement de X millions dans la prochaine année, est-ce trop ou trop peu?

Améliorer la communication

CA | CD | CE | CI | CGR | RSSI | Société

Je sais que les cyberrisques sont complexes en raison des nombreuses interdépendances – comment pouvons-nous obtenir un portrait clair de notre exposition globale afin de prendre des décisions efficaces et éclairées?

Se conformer à la réglementation

Org. de régl. | CA | CD | CGR | RSSI

Comment puis-je déterminer les répercussions potentielles « importantes » d'une cyberattaque sur mon entreprise? Comment puis-je communiquer au conseil d'administration de l'information sur les cyberrisques qui soit conforme aux nouvelles exigences en matière de rapports?

Principaux avantages

La solution vous fournit les outils pour :

Convaincre le conseil d'administration
Notre approche logique et transparente vous aide à bien exposer les cyberrisques aux parties prenantes, à démontrer les avantages de renforcer les cybercapacités et à présenter des dossiers d'investissement convaincants.

Effectuer des évaluations méthodiques, uniformes et fondées sur les données
Notre approche facilite et accélère l'adoption de techniques quantitatives et rend les évaluations des risques plus objectives grâce à des résultats cohérents et fondés sur les données.

Quantifier la probabilité et l'impact
Vous avez accès à des modèles éprouvés qui évaluent la probabilité d'occurrence des scénarios, la possibilité que les attaquants franchissent les différentes couches de défense et les pertes financières potentielles.

Cibler les dépenses pour réduire les risques
Nos modèles graphiques de scénarios de risque vous aident à voir où vos cybercapacités contribuent à réduire les risques aux différents niveaux de défense et quels domaines bénéficieraient le plus d'un investissement.

Optimiser les investissements
Déterminer le portefeuille optimal en matière de cybercapacités vous aidera à rentabiliser les investissements effectués pour réduire les risques.

Valider les investissements
Le délai de rentabilisation d'un investissement ou d'un portefeuille d'investissements sera estimé sur la base d'une analyse coûts-avantages des dépenses par rapport à la réduction attendue des pertes liées aux cyberattaques.

Communiquez avec nous pour discuter des besoins de votre organisation ou planifier une démonstration de la solution CRI.

Contacts

Paul Sammut
KPMG au Canada
Leader, Cyber Risk Insights
paul.sammut@kpmg.ca

Yassir Bellout
KPMG au Canada
Leader, Cyber Risk Insights
ybellout@kpmg.ca

Jason Flannery
KPMG au Canada
Spécialiste, Cyber Risk Insights
jasonflannery@kpmg.ca

Comment la solution CRI a-t-elle aidé nos clients?

Exemples des avantages dont ont profité des organisations de divers secteurs :

Confiance du conseil d'administration et réduction des risques — Détail

Pour tenir son engagement à se conformer à la norme ISO27001, l'entreprise avait tenté de s'attaquer sur tous les fronts en même temps, ce qui dépassait largement sa capacité de changement. La solution a permis de :

- ✓ réduire de 20 % les contrôles ISO27001 en se fondant sur la modélisation des attaques et la capacité d'analyse par simulation;
- ✓ réaliser des économies de plus de 850 000 $ et de prendre des décisions valables en matière de priorisation;
- ✓ se doter d'un système de mesure continue de l'exposition aux cyberrisques.

Hiérarchisation de la feuille de route — Assurance

Le conseil d'administration remettait en question les avantages du programme de cyberinvestissements présenté par le RISS et exigeait une réduction des dépenses. La solution a permis de :

- ✓ déterminer les investissements qui devaient faire l'objet de contrôles prioritaires en se fondant sur une analyse coût-avantages exhaustive;
- ✓ démontrer la réduction réelle des cyberrisques sur un an découlant des initiatives de suivi des changements;
- ✓ réaliser une évaluation détaillée de chaque unité opérationnelle suivant l'évaluation globale du groupe.

Gestion du risque dans l'ensemble d'un portefeuille — Placements privés

Plus de 20 sociétés du portefeuille nécessitaient une évaluation des cyberrisques et la mise en place d'un plan de redressement. La solution a permis :

- ✓ à chaque entreprise du portefeuille de chiffrer son exposition aux cyberrisques;
- ✓ à chaque entreprise de hiérarchiser ses investissements en cybersécurité en fonction des menaces spécifiques auxquelles ses activités sont exposées;
- ✓ de remplacer la méthode d'évaluation de la maturité (niveaux 1 à 5) en place, améliorant la confiance des dirigeants dans la sécurité du portefeuille.

Que faut-il attendre d'une évaluation CRI?

En général, une évaluation CRI se déroule en quatre étapes.

01 — Semaine 1

Délimitation de l'étendue

- Formulation de questions auxquelles l'organisation doit répondre.
- Identification des sources de données potentielles au sein de l'organisation pour compléter les ensembles de données de KPMG.

02 — Semaines 2 et 3

Sélection des scénarios de cybermenaces

- Détermination et modélisation de l'arbre d'attaque des scénarios prioritaires, accélérées par la bibliothèque de modèles de scénarios existante de KPMG.

03 — Semaines 3 à 6

Estimation et mesure

- Estimation et mesure des intrants nécessaires à l'élaboration des modèles de quantification des cyberrisques de KPMG.

04 — Semaines 4 à 8

Analyse et rapports

- Production de rapports indiquant les résultats en réponse aux questions posées à l'étape1.
- Nous accompagnerons vos principales parties prenantes dans leur parcours de communication de l'information, en veillant à ce qu'elles puissent adhérer rapidement à une approche axée sur les rapports quantitatifs.

kpmg.com.ca/fr