Cyber-assurance

RAPPORT D'ÉVALUATION RÉSUMÉ

Préparé à l'attention de

<NOM DU CLIENT ICI>

Industrie verticale : Finances et assurances
Région (s): Canada, États-Unis, Europe et Russie, Australie et Nouvelle-Zélande, Asie centrale et du Sud, Asie de l'Est et Pacifique, Mexique, Amérique centrale et Caraïbes, Amérique du Sud, Moyen-Orient et Afrique du Nord
Revenu annuel : 52 000 000 000 $
Type de dossiers : PII, PCI, PHI

17 mai 2018

Présentation du rapport sur les cyber-risques

Nous vous remercions de l'intérêt que vous portez à la cyber-assurance d'AIG. Vous trouverez ci-joint un rapport que les proposants peuvent recevoir en conjonction avec le processus de proposition de la cyber-assurance. Ce rapport résume uniquement les résultats de l'évaluation par AIG des risques de votre compte en fonction de la proposition que vous avez soumise et de la connaissance du paysage du cyber-risque d'AIG. Si vous faites le choix de souscrire une cyber-assurance auprès d'AIG, vous avez la possibilité de recevoir un rapport plus long et plus détaillé qui comprend des données comparatives et qui peut vous aider à identifier les principales mesures de contrôle pouvant réduire les risques de votre organisation.

Nous serons heureux de vous mettre en relation avec certains des meilleurs spécialistes au monde en cybersécurité, droit et relations publiques pour vous aider à protéger votre organisation contre les atteintes à la protection des données sensibles, le piratage informatique, les erreurs des employés et l'inconnu. Si un sinistre se produit, nos spécialistes internes en cyber-sinistres seront prêts à vous aider. Des outils de prévention des sinistres novateurs à la résolution de violations, nous nous engageons à vous aider à demeurer à l'avant-garde.

Évaluation AIG du cyber-risque

Dans le cadre du processus de souscription, AIG évalue le cyber-risque en utilisant un modèle fondé sur une méthode brevetée pour laquelle AIG détient une licence, qui permet de mesurer et de modéliser le cyber-risque en termes économiques. AIG extrait les connaissances et les renseignements de nombreux ensembles de données et des réponses spécifiques de chaque client (provenant du questionnaire de cyber-assurance d'AIG) en :

- mesurant chaque mois la probabilité de menaces provenant de sources internes et externes, et en utilisant les données mises à jour dans la modélisation ;
- mesurant et modélisant la force des contrôles et leur incidence sur l'entreprise ;
- mesurant les cotes de risques résiduels, les principaux scénarios de risque, la mise en œuvre des contrôles et les directives de restauration par ordre de priorité ;
- estimant l'incidence, la probabilité d'un cyber-incident et la portée de pertes prévues.

Ce rapport ne doit pas être considéré comme une évaluation complète des cyber-risques. Les réponses subjectives, fournies par le client dans la proposition de cyber-assurance d'AIG, peuvent ne pas être exactes. En raison des menaces émergentes et autres variables en évolution, l'exactitude de ce rapport diminue au fil du temps. En outre, les valeurs de l'incidence et les valeurs de probabilité sont calculées sur la base des échelles et des courbes statistiques et dérivées connues. En tant que tel, un client pourrait se situer en dehors de l'échelle ou de la courbe en raison de l'incertitude.

Résumé rapide des cotes

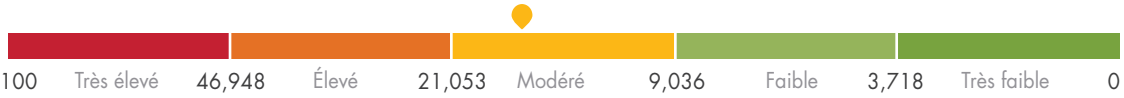
Cyber-maturité

L'état de préparation d'une organisation contre les cyber-menaces et sa capacité à protéger ses actifs informationnels.

42,53%
En développement

Risque résiduel

La combinaison rémanente de la menace et du risque d'incidence associés à une organisation, en tenant compte des bénéfices des contrôles en place en matière de cybersécurité



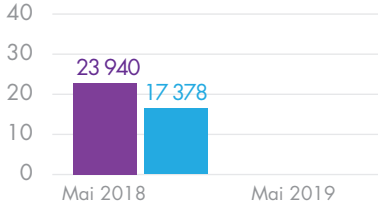
13,757
Modéré

Probabilité de menace

La probabilité d'une action malveillante ou non intentionnelle pouvant révéler une ou plusieurs faiblesses au sein de l'écosystème informatique d'une organisation.

3,887
Modéré

Tendance de base du risque



Risque implicite

Risque résiduel

**Remarque : les prochains rapports illustreront les tendances d'une évaluation à l'autre. S'agissant de la première évaluation, seule la tendance de base du risque implicite (inhérent) au risque résiduel est illustrée.*

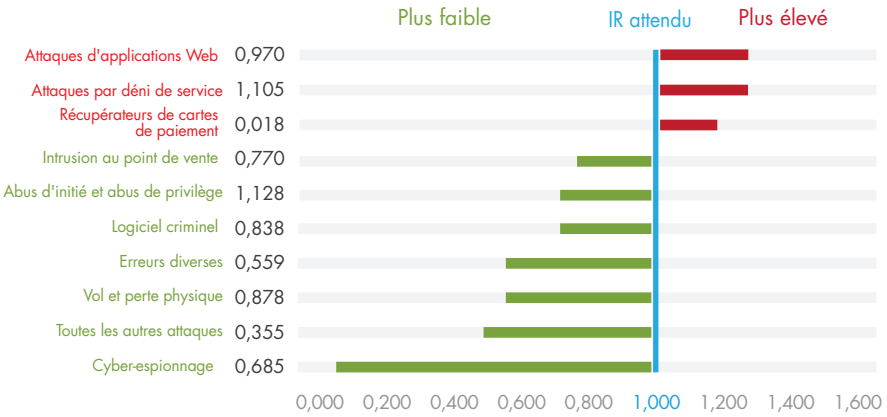
La combinaison de la menace et du risque d'incidence associés à une organisation, sans tenir compte des avantages des contrôles en matière de cybersécurité.

Les 5 principaux scénarios de risques

Classement	Scénario de risque
1	Abus d'initié et abus de privilège : serveurs et applications
2	Attaques par déni de service: serveurs et applications
3	Attaque par déni de service : Réseau
4	Attaques d'applications Web : serveurs et applications
5	Vol et perte physique : systèmes d'utilisateur final

Indice de risque par catégorie de menace

Il s'agit d'une mesure de la valeur de risque de l'organisation associée à chacune des catégories de menaces applicables par rapport à la valeur de risque moyenne prévue pour cette catégorie de menaces parmi toutes les organisations. Un indice de risque supérieur à 1,000 indique que l'organisation est particulièrement à risque dans cette catégorie de menaces. Un indice de risque pourrait être supérieur à 1,000 car la menace est accrue pour le secteur d'activité de l'organisation, l'entreprise est particulièrement sensible à l'incidence de cette menace, la mise en œuvre des contrôles de l'organisation ne traite pas cette menace, ou une combinaison des trois. En classant les menaces par leur cote d'indice de risque, de la plus élevée à la plus basse et en comparant leur amplitude relative, une organisation peut mieux comprendre les menaces auxquelles elle fait face.



**Remarque : dans le graphique ci-dessus, 1.0 est la valeur d'indice de risque attendue. Si une valeur est supérieure à 1,0, le risque est plus élevé que prévu. Si une valeur est inférieure à 1,0, le risque est plus faible que prévu.*

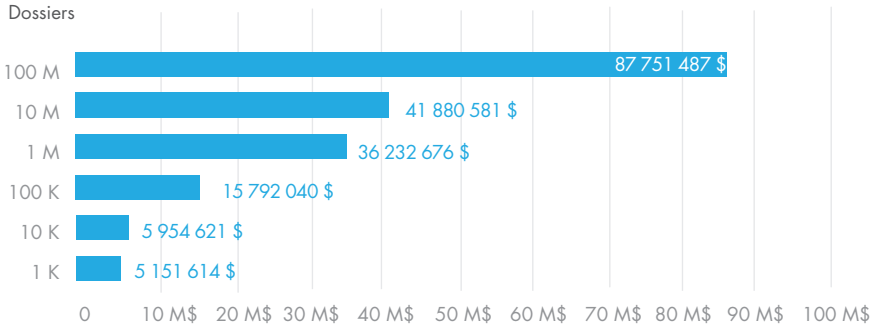
Les 5 principaux contrôles de réduction des risques

Il s'agit d'une liste par ordre de priorité des contrôles de sécurité critiques du Center for Internet Security (CIS) pour une cyberdéfense efficace, avec les principales mesures qui réduiraient le mieux la cote globale de risque résiduel de l'organisation listées en premier lieu. En mettant en œuvre les contrôles qui correspondent à ces mesures clés, une organisation peut améliorer sa cote de risque résiduel. Remarquez que tout changement dans l'environnement des menaces peut redéfinir l'ordre de priorité de ces recommandations.

Classement	Contrôle de sécurité critique de CIS
1	19. Gestion et réponse aux incidents
2	17. Évaluation des compétences en matière de sécurité et formation appropriée pour combler les lacunes
3	13. Protection des données
4	14. Accès contrôlé fondé sur le besoin de savoir
5	12. Défenses des limites

Incidence de la violation des données

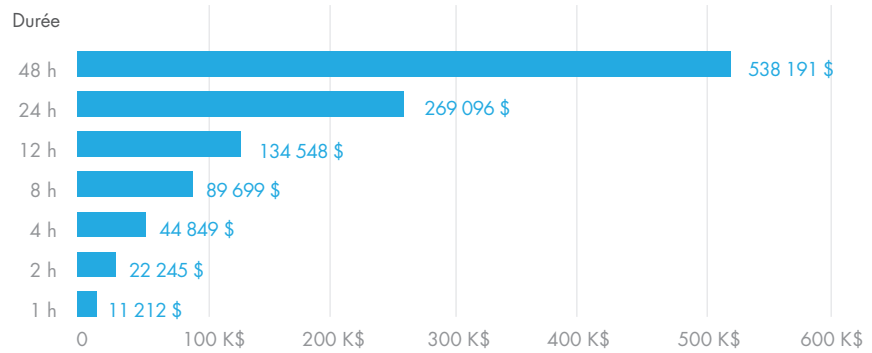
(valeur moyenne d'incidence par volume de dossiers)



Volume de violation *(Dossiers)*	Violation de faible incidence	Violation à incidence élevée	Pire scénario de violation
100 M	33 128 015 $	174 201 553 $	547 863 884 $
10 M	12 490 830 $	92 277 608 $	290 213 078 $
1 M	4 709 956 $	34 795 404 $	109 431 544 $
100 K	1 775 958 $	13 120 118 $	41 262 770 $
10 K	669 670 $	4 947 274 $	15 559 177 $
1 K	252 516 $	1 865 495 $	5 866 983 $

Incident d'interruption due à un déni de service

(Valeur de l'impact moyen par heure)



Durée d'interruption	Interruption à faible incidence	Interruption à incidence élevée	Pire cas d'interruption
48 h	76 451 745 $	335 106 366 $	492 043 011 $
24 h	38 225 873 $	167 553 183 $	246 021 505 $
12 h	28 669 405 $	125 664 887 $	184 516 129 $
8 h	19 112 936 $	83 776 591 $	123 010 753 $
4 h	15 927 447 $	69 813 826 $	102 508 961 $
2 h	12 741 958 $	55 851 061 $	82 007 168 $
1 h	9 556 468 $	41 888 296 $	61 505 376 $