Cyber-assurance

RAPPORT SOMMAIRE

Préparé à l'attention de

NOM DU CLIENT ICI

Industrie verticale	Finances et assurances
Région (s)	Canada, États-Unis, Europe, Russie et Afrique du Sud
Revenu annuel	136 000 000 $
Type de dossiers	PII, PCI

4 octobre 2018

Présentation du rapport sur les cyber-risques

Nous vous félicitons d'avoir souscrit à la cyber-assurance d'AIG. En votre qualité de titulaire de police ayant rempli le processus de proposition de la cyber-assurance, vous et votre organisation avez fait le choix de recevoir le rapport sommaire suivant. Celui-ci fournit des renseignements supplémentaires à partir 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 avez des questions concernant votre rapport sommaire, veuillez contacter votre souscripteur en cyber-assurance AIG, ou nous envoyer un courriel à CyberRiskConsulting@aig.com.

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 réponses spécifiques des clients (provenant de la proposition de cyber-assurance d'AIG) en :

- mesurant chaque mois la probabilité de menaces internes et externes 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 les portées 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 la 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 l'échelle en raison de l'incertitude.

Résumé des Cyber-risques

Cyber-maturité

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

37,39%
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 matière de cybersécurité.

35,75
Élevé

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.

5,052
Élevé

Efficacité des contrôles

indique dans quelle mesure chaque contrôle réduit le risque, en fonction de la manière dont les contrôles sont mis en œuvre.

48.75
Importante

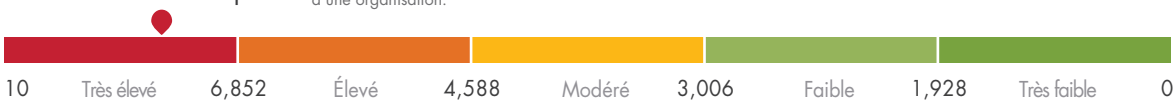
Risque implicite

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.

37.749
Élevé

Incidence sur l'entreprise

Le degré associé aux actifs concernés de confidentialité, d'intégrité et de répercussion sur la disponibilité au sein d'une organisation.



7.952
Très élevé

Pratiques par ordre de priorité

Il s'agit de la liste des principales pratiques de réduction des risques identifiés dans la proposition de cyber-assurance d'AIG que le client n'a pas encore mises en œuvre. Cette liste est fondée sur la probabilité actuelle de menaces, tel qu'indiqué dans la section Détails de la probabilité des menaces de ce rapport et peut varier en cas de changement du contexte des menaces. Les valeurs de l'indice à droite mesurent la réduction du risque résiduel associée à la mise en œuvre de chaque pratique par rapport à la pratique ayant la qualité de réduction du risque la plus élevée.

Classement	Section Questionnaire	Sous-section du questionnaire	Numéro de question	Description de la question	Indice de qualité de la réduction des risques relatifs
1	Contrôle	Général	15	Contrôle des modifications	*
2	Contrôle	DoS	1	Atténuation DoS	0,202
3	Contrôle	Serveur/Applications	2	Solution DLP	0,148
4	Contrôle	s.o.	11	Certification PCI DSS	0,147
5	Contrôle	WebApp	13	Réponse aux incidents	0,129
6	Contrôle	WebApp	12	Cycle de vie des applications et révision du code	0,112
7	Contrôle	WebApp	9	Authentification multifactorielle et droit d'accès minimal	0,105
8	Contrôle	WebApp	1	Détection des ressources	0,102
9	Contrôle	Général	16	Authentification multifactorielle	0,100
10	Contrôle	Serveur/Applications	7	Authentification multifactorielle	0,096

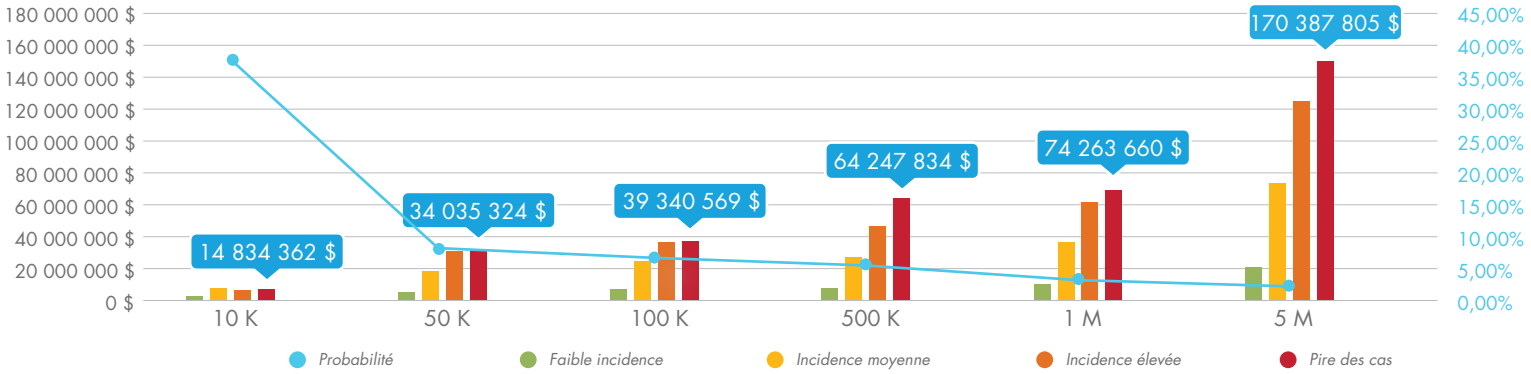
Remarque : il n'y a soit pas eu de réponses enregistrées aux questions ci-dessus au cours du processus de proposition, ou les réponses ont été données d'une manière laissant à penser que la ou les pratiques pourraient ne pas être entièrement mises en œuvre.

Violation des données : probabilité et incidence du cyber-incident

VIOLATION DES DONNEES PERTE PRÉVUE
15,3 millions $
(Violation - scénario d'incidence moyenne)

PROBABILITÉ DE VIOLATION DES DONNÉES
0,23%
(5 millions de dossiers)

VIOLATION DES DONNÉES PIRE SCÉNARIO
170, 38 millions $
(5 millions de dossiers)



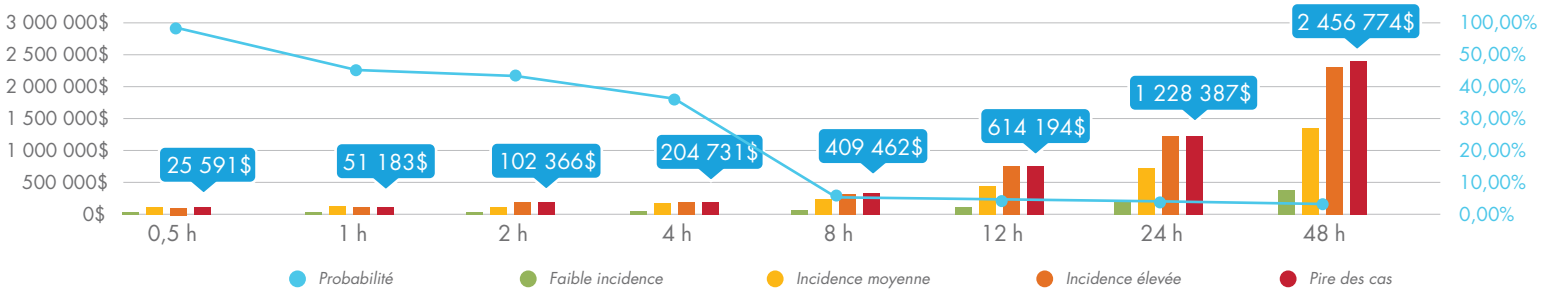
Volume de violation (Dossiers)	Probabilité	Violation de faible incidence	Violation à incidence moyenne	Violation à incidence élevée	Pire scénario de violation
10 K	38,288%	579 187 $	2 647 998 $	4 716 808 $	14 834 362 $
50 K	8,432%	1 328 862 $	6 075 452 $	10 822 043 $	34 035 324 $
100 K	1,935%	1 535 998 $	7 022 461 $	12 508 925 $	39 340 569 $
500 K	1,057%	3 524 170 $	11 976 367 $	20 428 564 $	64 247 834 $
1 M	0,756%	4 073 566 $	13 843 406 $	23 613 246 $	74 263 660 $
5 M	0,235%	9 346 240 $	31 761 801 $	54 177 362 $	170 387 805 $

Interruption due à un déni de service : probabilité et incidence du cyber-incident

INTERRUPTION PERTE PRÉVUE
102 000 $
(Attaque DoS - scénario d'incidence moyenne)

PROBABILITÉ D'INTERRUPTION
2,31%
(Attaque DoS - 48 heures)

PIRE SCENARIO D'INTERRUPTION
2,45 million $
(Attaque DoS - 48 heures)



Durée d'interruption (heures)	Probabilité	Interruption à faible incidence	Interruption à incidence moyenne	Interruption à incidence élevée	Pire cas d'interruption
0.5 h	98,70%	2 083 $	5 606 $	9 130 $	25 591 $
1 h	45,19%	4 166 $	11 212 $	18 259 $	51 183 $
2 h	43,83%	8 331 $	22 425 $	36 518 $	102 366 $
4 h	38,43%	16 663 $	44 849 $	73 036 $	204 731 $
8 h	4,42%	33 325 $	89 699 $	146 072 $	409 462 $
12 h	3,34%	49 998 $	134 548 $	219 108 $	614 194 $
24 h	2,75%	99 975 $	269 096 $	438 216 $	1 228 387 $
48 h	2,31%	199 951 $	538 191 $	876 432 $	2 456 774 $

Détails du risque résiduel

Le risque résiduel est le reste du risque associé à une organisation. Il représente les avantages de la mise en œuvre des contrôles de cybersécurité de réduction des risques.
La cote de risque résiduel pour < Nom du client Ici > est de 35,75, ce qui est élevé.

	Attaques d'applications Web	Intrusion au point de vente	Abus d'initié et abus de privilège	Erreurs diverses	Vol et perte physique	Logiciel criminel	Récupérateurs de cartes de paiement	Cyber espionnage	Attaques par déni de service	Toutes les autres attaques
Serveurs et applications	29,100	16,205	14,213	8,955	0,389	13,580	0,530	10,580	28,664	8,445
Réseau	6,900	6,429	9,597	4,995	0,393	7,702	0,512	6,142	22,118	4,569
Systèmes d'utilisateur final	11,706	15,819	11,330	6,179	10,578	11,268	6,638	8,932	6,654	6,961
Terminal	19,825	16,098	11,652	1,370	0,339	6,358	24,014	6,992	5,452	4,196
ICS/SCADA/OT	23,533	0,000	16,057	10,665	0,398	15,849	0,633	12,515	26,387	10,136
Appareils de soins de santé	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Systèmes embarqués	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
IdO critique	9,318	14,696	12,907	2,374	3,162	12,720	6,596	7,652	6,451	4,694
IdO non critique	4,840	0,000	5,373	0,566	0,145	2,788	0,215	3,394	2,538	1,963
Médias et Données hors ligne	0,677	2,570	10,042	3,856	4,567	0,711	0,651	1,181	0,797	0,889
Personnes	11,287	4,561	13,890	8,707	5,411	9,845	0,844	6,337	6,867	6,824

Remarque : dans le graphique ci-dessus, les valeurs 0,000 signifient que le scénario de risque n'est pas applicable pour le profil du client. La couleur de la cellule représente le degré de risque résiduel. Plus la cellule est foncée, plus le risque résiduel est élevé.

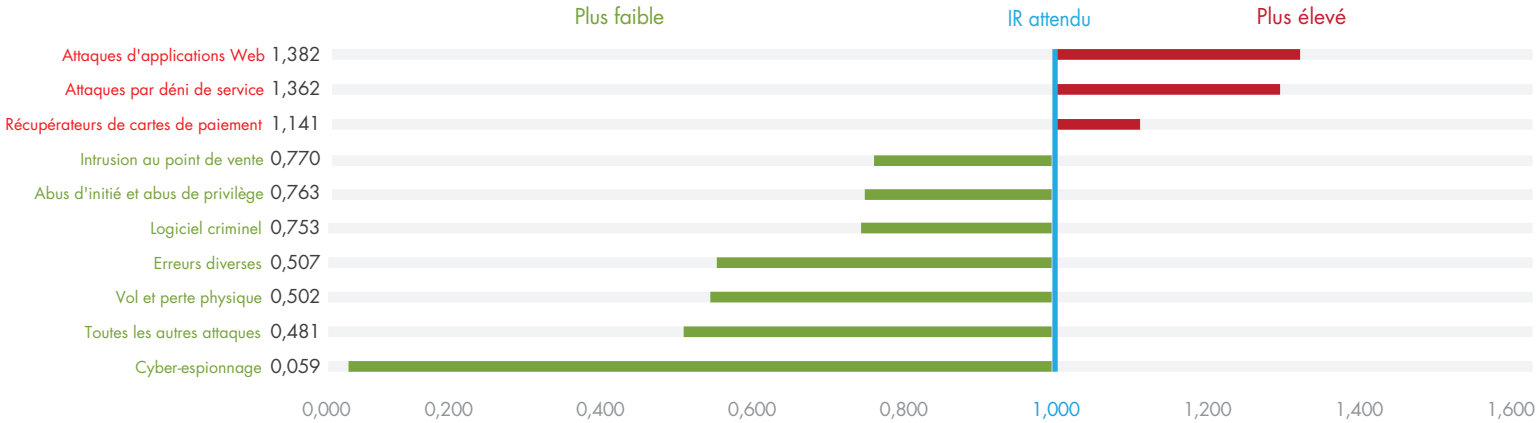
Les 10 principaux scénarios de risque résiduel

Classement	Scénario de risque résiduel	Cote de risque résiduel	Échelle de risque résiduel
1	Attaques d'applications Web: serveurs et applications	29,100	Élevé
2	Attaques par déni de service: serveurs et applications	28,644	Élevé
3	Attaques par déni de service: ICS/SCADA/OT	26,387	Élevé
4	Récupérateurs de cartes de paiement: terminal	24,014	Élevé
5	Attaques d'applications Web: ICS/SCADA/OT	23,533	Élevé
6	Attaques d'applications Web: Terminal	19,825	Modéré
7	Intrusion au point de vente : serveurs et applications	16,205	Modéré
8	Intrusion au point de vente : Terminal	16,098	Modéré
9	Abus d'initié et abus de privilège : ICS/SCADA/OT	16,057	Modéré
10	Logiciel criminel : ICS/SCADA/OT	15,849	Modéré

Remarque : les 10 principaux scénarios de risque résiduel sont tirés directement de la grille des risques résiduels ci-dessus et peuvent être utiles pour hiérarchiser les décisions de remédiation et de transfert des risques.

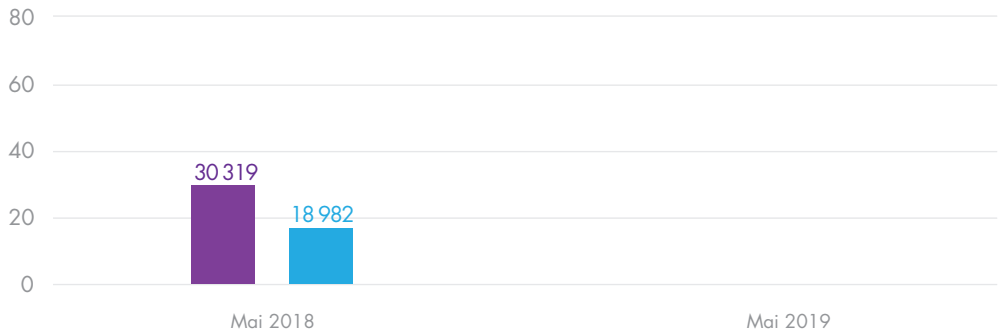
Indice de risque par catégorie de menaces

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 un niveau de risque accru pour une organisation dans cette catégorie de menaces. Un indice de risque pourrait être supérieur à 1,000 en raison d'une menace accrue pour le secteur d'activité de l'organisation, de la sensibilité de l'entreprise à l'incidence de cette menace, d'une faiblesse dans la mise en œuvre des contrôles de l'organisation à l'égard de 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 le risque que constituent les différentes menaces.



Remarque : dans le graphique ci-dessus, 1,000 est la valeur d'indice de risque attendue. Si une valeur d'indice de risque est supérieure à 1,000, le risque est plus élevé que prévu. Si une valeur d'indice de risque est inférieure à 1,000, le risque est plus faible que prévu.

Tendance de base du risque



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.

Risque implicite 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

Risque résiduel La combinaison rémanente de menace et de risque d'incidence associés à une organisation, en tenant compte des avantages des contrôles en matière de cybersécurité.

Détails de la probabilité des menaces

La probabilité d'une menace est la probabilité d'une action malveillante ou non intentionnelle, qui pourrait révéler des faiblesses au sein de l'écosystème des technologies de l'information d'une organisation. La cote de probabilité d'une menace pour < Nom du client Ici > est de 5,052, ce qui est élevé.

	Attaques d'applications Web	Intrusion au point de vente	Abus d'initié et abus de privilège	Erreurs diverses	Vol et perte physique	Logiciel criminel	Récupérateurs de cartes de paiement	Cyber espionnage	Attaques par déni de service	Toutes les autres attaques
Serveurs et applications	9,991	2,979	4,470	2,755	0,102	4,457	0,128	3,427	9,000	2,772
Réseau	2,460	1,488	2,966	1,536	0,102	2,364	0,128	1,885	6,750	1,378
Systèmes d'utilisateur final	4,769	2,978	4,367	2,320	3,506	4,457	1,655	3,532	2,250	2,753
Terminal	7,204	2,977	4,192	0,458	0,102	2,369	6,618	2,585	1,800	1,564
ICS/SCADA/OT	6,953	0,968	4,209	2,580	0,102	4,268	0,128	3,353	6,300	2,730
Appareils de soins de santé	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Systèmes embarqués	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
IdO critique	3,213	2,663	4,226	0,719	0,903	4,314	1,655	2,585	1,980	1,587
IdO non critique	3,464	0,895	4,159	0,405	0,102	2,235	0,128	2,710	1,890	1,569
Médias et Données hors ligne	0,251	0,647	3,988	1,642	1,771	0,157	0,128	0,447	0,174	0,336
Personnes	4,016	0,951	4,900	2,765	1,736	3,127	0,128	2,013	2,430	2,168

Remarque : dans le graphique ci-dessus, les valeurs 0,000 signifient que le scénario de risque n'est pas applicable pour le profil du client. La couleur de la cellule représente le degré de probabilité de la menace. Plus la cellule est foncée, plus la probabilité de la menace est élevée.

Résumé des menaces :

1. Référence de l'industrie: le profil de la probabilité de la menace a été créé à partir d'une référence objective du secteur (< SECTEUR D'ACTIVITÉ DU CLIENT >) et des propositions de cyber-assurance d'AIG.
2. Applicabilité: le < NOMBRE D'ACTIFS > des 11 groupes d'actifs se rapporte à < < NOM DU CLIENT > >.
3. La menace principale : < MENACE PRINCIPALE > est la catégorie de menaces la plus probable.

Remarque : AIG déconseille de prendre des décisions en matière d'atténuation ou de transfert des cyber-risques uniquement à partir des détails des menaces contenus dans cette section du rapport.

Détails de l'efficacité des contrôles

L'efficacité du contrôle est l'avantage synergique de la réduction des risques qu'apportent les contrôles de cybersécurité en fonction de la manière dont ils sont mis en œuvre.
La cote d'efficacité des contrôles pour < Nom du client ici > est de 48,75, ce qui est IMPORTANT.

	Attaques d'applications Web	Intrusion au point de vente	Abus d'initié et abus de privilège	Erreurs diverses	Vol et perte physique	Logiciel criminel	Récupérateurs de cartes de paiement	Cyber espionnage	Attaques par déni de service	Toutes les autres attaques
Serveurs et applications	57,72	15,89	57,05	56,10	52,73	58,84	43,90	58,30	60,43	58,84
Réseau	58,91	32,55	54,75	54,51	52,20	54,45	43,90	54,44	57,29	53,64
Systèmes d'utilisateur final	57,51	17,05	57,48	56,35	53,46	58,57	43,90	58,56	61,45	58,57
Terminal	57,04	15,57	57,03	53,69	52,73	58,51	43,90	58,17	60,51	58,51
ICS/SCADA/OT	57,33	15,86	56,82	53,20	52,73	57,97	43,90	57,76	58,12	57,97
Appareils de soins de santé	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Systèmes embarqués	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
IdO critique	57,27	15,57	57,03	53,55	52,73	58,51	43,90	58,34	60,51	58,38
IdO non critique	57,27	15,57	57,03	53,55	52,73	58,51	43,90	58,34	60,51	58,38
Médias et Données hors ligne	44,18	14,49	50,59	53,93	51,78	11,20	0,00	48,14	0,00	48,14
Personnes	52,89	16,94	57,08	52,33	51,92	52,34	0,00	52,34	58,76	52,34

Remarque : dans le graphique ci-dessus, les valeurs 0,000 signifient que le scénario de risque n'est pas applicable pour le profil du client. La couleur de la cellule représente le degré d'efficacité des contrôles. Plus la cellule est foncée, plus l'efficacité du contrôle est élevée.

Contrôles de sécurité critiques (CSC) du CIS Cote d'alignement

La cote d'alignement des contrôles de sécurité critiques du CIS est une mesure de la mise en œuvre par l'organisation des contrôles de sécurité critiques du Center for Internet Security (CIS) pour une cyberdéfense efficace, combinée à la qualité de ces contrôles dans la réduction synergique des risques. Cette cote n'est pas une mesure de la conformité. Veuillez noter qu'il n'y a pas nécessairement de corrélation entre la cote d'alignement d'un contrôle précis et les scénarios individuels présentant le risque résiduel le plus important pour < NOM DU CLIENT ICI >. La mise en œuvre d'un contrôle ayant la cote d'alignement la plus basse ne garantit pas d'obtenir la plus grande réduction du risque résiduel agrégé. Au contraire, < NOM DU CLIENT ICI > devrait envisager d'accorder la priorité aux contrôles ayant la « qualité de réduction du risque agrégé restant » la plus importante.

Contrôle	Cote	Nom du contrôle
1	48,32%	Inventaire des périphériques autorisés et non autorisés
2	68,22%	Inventaire des logiciels autorisés et non autorisés
3	48,32%	Configuration sécurisée pour le matériel informatique et les logiciels
4	59,09%	Évaluation continue de la vulnérabilité et correction
5	58,49%	Utilisation contrôlée des privilèges d'administration
6	56,75%	Maintenance, surveillance et analyse des journaux d'audit
7	64,96%	Protections de courriel et de navigateur Web
8	62,55%	Défenses contre les logiciels malveillants
9	63,76%	Limitation et contrôle des ports réseau
10	71,06%	Capacité de récupération de données
11	64,38%	Configurations sécurisées pour les périphériques réseau
12	53,59%	Défenses des limites
13	26,28%	Protection des données
14	48,32%	Accès contrôlé fondé sur le besoin de savoir
15	56,18%	Contrôle d'accès sans fil
16	56,45%	Surveillance et contrôle des comptes
17	37,95%	Évaluation des compétences en matière de sécurité et formation pour combler les lacunes
18	52,38%	Sécurité des logiciels d'application
19	59,09%	Gestion et réponse aux incidents
20	42,21%	Tests de pénétration et exercices d'équipe rouge (Red Team)

Indice de qualité de la réduction du risque agrégé restant

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, dans l'ordre dans lequel chaque contrôle de sécurité réduirait les cotes de risque des 110 scénarios de risque applicables pour < Nom du client ici >, en supposant que le contrôle a été pleinement mis en œuvre et qu'il n'y a eu aucun changement de probabilité des menaces. Les valeurs d'indice à droite fournissent une mesure relative de l'effet de chaque contrôle de sécurité sur le risque résiduel. Bien que cette analyse ne comprenne pas le coût de la mise en œuvre intégrale des contrôles, l'organisation peut combiner ces données avec le coût relatif pour hiérarchiser les améliorations à apporter aux contrôles.

Classement	Nom du contrôle	Index
1	13. Protection des données	*
2	14. Accès contrôlé fondé sur le besoin de savoir	0,940
3	12. Défenses des limites	0,762
4	19. Gestion et réponse aux incidents	0,747
5	17. Évaluation des compétences en matière de sécurité et formation pour combler les lacunes	0,727
6	3. Configuration sécurisée pour le matériel informatique et les logiciels	0,726
7	1. Inventaire des périphériques autorisés et non autorisé	0,703
8	8. Défenses contre les logiciels malveillantss	0,701
9	9. Limitation et contrôle des ports réseau	0,695
10	5. Utilisation contrôlée des privilèges d'administration	0,686
11	7. Protections de courriel et de navigateur Web	0,643
12	2. Inventaire des logiciels autorisés et non autorisés	0,634
13	20. Tests de pénétration et exercices d'équipe rouge (Red Team)	0,550
14	4. Évaluation continue de la vulnérabilité et correction	0,534
15	16. Surveillance et contrôle des comptes	0,510
16	6. Maintenance, surveillance et analyse des journaux d'audit	0,475
17	11. Configurations sécurisées pour les périphériques réseau	0,398
18	15. Contrôle d'accès sans fil	0,370
19	10. Capacité de récupération de données	0,367
20	18. Sécurité des logiciels d'application	0,333

Risque implicite en détails

Le risque implicite est le risque global ou le risque inhérent associé à une organisation. Il s'agit purement de la combinaison de la menace et de l'incidence associées à une organisation. Il ne comprend pas les avantages des contrôles en matière de cybersécurité. La cote de risque implicite pour < Nom du client Ici > est de 37,749, ce qui est élevé.

	Attaques d'applications Web	Intrusion au point de vente	Abus d'initié et abus de privilège	Erreurs diverses	Vol et perte physique	Logiciel criminel	Récupérateurs de cartes de paiement	Cyber espionnage	Attaques par déni de service	Toutes les autres attaques
Serveurs et applications	68,826	19,268	33,092	20,398	0,822	32,994	0,946	25,369	72,437	20,518
Réseau	16,792	9,532	21,209	10,982	0,822	16,908	0,913	13,481	51,781	9,854
Systèmes d'utilisateur final	27,552	19,071	26,647	14,157	22,726	27,196	11,833	21,553	17,260	16,801
Terminal	46,143	19,066	27,113	2,959	0,717	15,323	42,807	16,716	13,808	10,113
ICS/SCADA/OT	55,156	0,000	37,186	22,788	0,842	37,707	1,128	29,626	62,999	24,115
Appareils de soins de santé	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Systèmes embarqués	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
IdO critique	21,807	17,406	30,034	5,112	6,688	30,657	11,758	18,366	16,338	11,278
IdO non critique	11,326	0,000	12,502	1,219	0,307	6,720	0,384	8,145	6,429	4,716
Médias et Données hors ligne	1,213	3,005	20,324	8,370	9,472	0,800	0,651	2,277	0,797	1,714
Personnes	23,959	5,491	32,365	18,266	11,254	20,657	0,844	13,297	16,650	14,317

Remarque : dans le graphique ci-dessus, les valeurs 0,000 signifient que le scénario de risque n'est pas applicable pour le profil du client. La couleur de la cellule représente le degré de risque implicite. Plus la cellule est foncée, plus le risque implicite est élevé.

Résumé des risques implicites :

1. Calcul du risque implicite : le risque implicite correspond simplement à la multiplication de la probabilité d'une menace et de son incidence sur l'entreprise.
2. Applicabilité: le < NOMBRE D'ACTIFS > des 11 groupes d'actifs se rapporte à < < NOM DU CLIENT > >.
3. Scénario de risque le plus élevé: en termes de risque implicite, le scénario qui présente le risque le plus grand pour < NOM DU CLIENT > est l'intersection du < SCHÉMA D'ATTAQUE DU SCÉNARIO DE RISQUE LE PLUS ÉLEVÉ> et de < L'ACTIF DU SCÉNARIO DE RISQUE LE PLUS ÉLEVÉ >.

Remarque : AIG déconseille de prendre des décisions en matière d'atténuation ou de transfert des cyber-risques uniquement à partir des détails des risques implicites contenus dans cette section du rapport.

Détails de l'incidence sur l'entreprise

L'incidence sur l'entreprise est le degré associé aux actifs concernés de confidentialité, d'intégrité et de répercussion sur la disponibilité au sein d'une organisation. La cote d'incidence sur l'entreprise pour < Nom du client ici > est de 7,952, ce qui est très élevé.

	Attaques d'applications Web	Intrusion au point de vente	Abus d'initié et abus de privilège	Erreurs diverses	Vol et perte physique	Logiciel criminel	Récupérateurs de cartes de paiement	Cyber espionnage	Attaques par déni de service	Toutes les autres attaques
Serveurs et applications	6,889	6,468	7,403	7,403	8,056	7,403	7,403	7,403	8,049	7,403
Réseau	6,826	6,405	7,151	7,151	8,056	7,151	7,151	7,151	7,671	7,151
Systèmes d'utilisateur final	5,777	6,405	6,102	6,102	6,482	6,102	7,151	6,102	7,671	6,102
Terminal	6,405	6,405	6,468	6,468	7,030	6,468	6,468	6,468	7,671	6,468
ICS/SCADA/OT	7,932	0,000	8,834	8,834	8,252	8,834	8,834	8,834	10,000	8,834
Appareils de soins de santé	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Systèmes embarqués	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
IdO critique	6,787	6,535	7,106	7,106	7,408	7,106	7,106	7,106	8,252	7,106
IdO non critique	3,270	0,000	3,006	3,006	3,006	3,006	3,006	3,006	3,402	3,006
Médias et Données hors ligne	4,834	4,645	5,096	5,096	5,350	5,096	5,096	5,096	4,588	5,096
Personnes	5,966	5,777	6,605	6,605	6,482	Lorem	6,605	6,605	6,852	6,605

Remarque : dans le graphique ci-dessus, les valeurs 0,000 signifient que le scénario de risque n'est pas applicable pour le profil du client. La couleur de la cellule représente le degré de l'incidence sur l'entreprise. Plus la cellule est foncée, plus l'incidence sur l'entreprise est élevée.

Résumé de l'incidence sur l'entreprise :

1. Profil de l'incidence sur l'entreprise : le profil de l'incidence sur l'entreprise a été élaboré à partir des réponses spécifiques dans la proposition de cyber-assurance d'AIG.
2. Applicabilité: le < NOMBRE D'ACTIFS > des 11 groupes d'actifs se rapporte à < < NOM DU CLIENT > >.
3. Groupe d'actifs le plus critique: en termes d'incidence sur l'entreprise, le <groupe d'actifs le plus critique> est le groupe d'actifs critiques le plus important.

Remarque : AIG déconseille de prendre des décisions en matière d'atténuation ou de transfert des cyber-risques uniquement à partir des détails de l'incidence sur l'entreprise contenus dans cette section du rapport.