MARKEL

Cyber 360 Canada

Markel Cyber 360 Canada

Nous avons conçu Cyber 360 Canada pour protéger les entreprises avant, pendant et après une cyberattaque, afin que vous soyez protégé et couvert.

Grâce à notre groupe d'experts, nous offrons une gamme de services de soutien lorsque vous en avez le plus besoin. Qu'il s'agisse d'interventions en cas d'atteinte à la sécurité des données, de gestion des incidents, de questions juridiques, d'enquêtes judiciaires, de surveillance du crédit, de gestion de centres d'appels, de limitation des pertes ou de relations publiques, nous sommes à vos côtés. En outre, notre service téléphonique de déclaration de sinistre offert 24 heures sur 24, 7 jours sur 7 vous permet de nous contacter en tout temps en cas de cyberattaque.

Sommaire de la couverture des risques propres :

– Frais de criminalistique informatique

– Frais de notification et d'atténuation des atteintes à la vie privée

– Frais de restauration des systèmes et des données

– Frais liés aux pertes d'exploitation

– Défaillance des systèmes

– Interruption des activités des fournisseurs de services essentiels

– Défaillance des systèmes des fournisseurs de services essentiels

– Frais liés à une extorsion

Extensions de garantie et avenants :

– Mises à niveau et remplacement du matériel informatique rendu inutilisable (« bricking »)

– Minage clandestin et fraude liée aux télécommunications

– Carence et défaillance des systèmes des fournisseurs de services autres qu'informatiques

– Fermeture réglementaire et volontaire

– Cybervol et ingénierie sociale

– Atteinte à la réputation

Sommaire de la couverture des tiers :

– Responsabilité civile liée aux cyberrisques et à la protection des renseignements personnels

– Enquêtes et amendes réglementaires

– Enquêtes et amendes relatives à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

– Responsabilité liée aux médias électroniques

Options de garanties supplémentaires :

– Responsabilité civile liée aux services professionnels et technologiques

– Responsabilité civile des administrateurs et des dirigeants

– Pratiques en matière d'emploi et responsabilité en matière de discrimination à l'égard des tiers

– Responsabilité à titre de fiduciaire

– Vol

MARKEL

Markel Cyber 360 Canada — Intervention en cas d'incident

Chez Markel, la **sécurité de nos clients est notre priorité.**

La transparence de notre gestion des atteintes à la sécurité des données est essentielle pour apaiser nos clients. Cela signifie qu'il faut établir des procédures simples et claires sur ce que vous devez faire — et ce que nous faisons — si le pire se produit.

Nous sommes à vos côtés dès que votre contrat est conclu. En cas de cyberurgence, une bonne préparation peut faire la différence entre la réparation rapide d'une atteinte à la sécurité des données et l'apparition d'un incident majeur.

En cas d'atteinte à la sécurité des données, notre équipe de consultants en intrusion informatique du cabinet d'avocats Norton Rose Fulbright agira rapidement, en suivant une approche simplifiée, afin de limiter les perturbations et de vous remettre sur pied.

Services en matière de cybersécurité de Norton Rose Fulbright :

Sous la direction d'Imran Ahmad et John Cassel, deux avocats ayant obtenu un classement du guide Chambers en 2025, Norton Rose Fulbright apporte une expertise exceptionnelle bilingue en matière de cybersécurité et de confidentialité des données, avec l'appui de la plus grande équipe spécialisée du Canada. En tant que conseillers de confiance des entreprises faisant partie du classement Fortune 100, ils jouent un rôle essentiel en aidant les organisations à se préparer de manière proactive aux cybermenaces et à y répondre de manière efficace.

Norton Rose Fulbright a conseillé des milliers de clients dans le monde entier sur la gestion des atteintes à la sécurité des données et des cyberincidents. L'équipe allie expertise sectorielle et portée internationale, car les atteintes à la sécurité des données ne connaissent pas de frontières. Cette équipe peut facilement faire appel à des partenaires spécialisés dans la protection de la vie privée et les interventions en cas d'atteinte à la sécurité des données au Canada et aux États-Unis, ainsi que dans plus de 50 villes réparties sur cinq continents.

- **Assistance bilingue 24 heures sur 24, 7 jours sur 7 et 365 jours par année.**
- **+1 000 cyberincidents traités à ce jour.**
- **Réseau de partenaires du domaine de la cybersécurité au Canada, en Amérique du Nord, en Europe, en Afrique, en Asie et en Australasie.**

MARKEL

FLUX DE TRAVAIL DES INTERVENTIONS EN CAS DE CYBERINCIDENTS

Chez Markel, la sécurité de nos clients cyberrisques est notre priorité.

La clé pour que nos clients se sentent rassurés est notre démarche transparente d'intervention en cas d'atteinte à la sécurité des données. Cela signifie qu'il faut établir des procédures simples et claires sur ce que vous devez faire — et ce que nous faisons — si le pire se produit.

Markel Cyber 360 Canada — Chronologie en cas d'atteinte à la sécurité des donnéese

01 — 1 HEURE

Atteinte à la sécurité des données soupçonnée — action initiale

Nos consultants en intrusion informatique agissent en tant qu'agents de notification et sont disponibles 24 heures sur 24, 7 jours sur 7, 365 jours par année. Les notifications peuvent être faites directement par l'intermédiaire de la ligne d'assistance téléphonique ou par courriel. Les coordonnées des personnes à contacter figurent également dans les politiques, ce qui permet aux assurés de les notifier directement.

Territoire

Lorsque l'assuré ou l'événement d'atteinte à la sécurité des données semble se situer au Québec, ils s'en remettront à la langue la plus appropriée.

Vérifications des conflits d'intérêts

Nos consultants en intrusion informatique reçoivent habituellement une réponse en moins d'une heure pendant les heures de bureau. Nos consultants en intrusion informatique ne tardent jamais à prendre le premier appel avec l'assuré. Si les résultats de la vérification ne sont pas accessibles, ils l'expliqueront à l'assuré.

Triage des incidents d'atteinte à la sécurité des données

Appel de triage pour identifier l'incident et déterminer l'étendue des services requis. Si aucun service n'est requis, nos consultants en intrusion informatique ne factureront pas le temps passé.

Lorsqu'une assistance supplémentaire est prévue, les consultants en intrusion informatique :

- Expliqueront le produit, les services et les coûts potentiels;
- Détermineront les services requis, y compris si une assistance canadienne ou étrangère est nécessaire, et détermineront le ou les sous-traitants appropriés pour apporter de l'aide;
- Offriront des conseils immédiats en matière de gestion du risque d'incident, y compris les premiers conseils juridiques sur les risques d'atteinte à la sécurité des données;
- Produiront un sommaire de la notification de l'incident et demanderont le consentement de l'assuré afin de le communiquer à l'assureur.

Si une assistance supplémentaire est nécessaire, les consultants en intrusion informatique :

- Enverront une lettre d'engagement à l'assuré, comprenant des dispositions relatives à la prestation des services par les sous-traitants;
- Produiront un rapport à l'intention de l'assuré décrivant la discussion, les options et les prochaines étapes;
- Convoqueront un appel supplémentaire avec le groupe de fournisseurs experts en cybersécurité qui aura lieu dans un délai de 2 heures.

02 — 24 HEURES

Analyse, rapports et gestion des atteintes à la sécurité des données

- Le consultant en intrusion informatique fournit des services au nom de l'assuré.
- Tous les fournisseurs spécialisés en cybersécurité coordonnés par nos consultants en intrusion informatique expliqueront l'étendue de leurs services à l'assuré.
- Collaboration avec des consultants en informatique pour contenir les incidents, enquêter sur ceux-ci et y remédier.
- PPrestation de conseils juridiques sur les questions réglementaires et juridiques découlant de l'incident, notamment la question de savoir si des notifications de l'autorité réglementaire compétente sont nécessaires.
- Fourniture à l'assuré d'un rapport d'incident dans les 24 heures.
- Examen afin de déterminer si des notifications immédiates sont nécessaires (par exemple, du responsable du traitement des données au contrôleur des données ou si des réglementations sectorielles l'exigent).
- Évaluation continue de l'opportunité de faire appel à d'autres sous-traitants (par exemple, des négociateurs dans le contexte de rançongiciels).

MARKEL

03

24 à 72 HEURES

Mesures d'atténuation et enquête

- Offre combinée de services juridiques et de services de gestion des risques liés à l'incident.
- Conseils sur les enjeux d'atteinte à la sécurité des données et les notifications potentielles aux organismes de réglementation ou aux personnes visées par ces données.
- Conseils sur d'autres questions juridiques, y compris les mesures de protection en cas de litige et la gestion de la réputation.
- Dirigés par nos consultants en intrusion informatique, les consultants en informatique effectuent habituellement la restauration et l'enquête en continu.
- Sous la direction de nos consultants en intrusion informatique, d'autres membres du groupe de fournisseurs spécialisés en cybersécurité offrent des services tels que la préparation de communiqués de presse, la formulation de communications de notification et la mobilisation d'agents de notification et de fournisseurs de services de surveillance du crédit.

04

72 HEURES+

Conclusion

- Les consultants en intrusion informatique continuent à fournir des services de gestion intégrée des risques combinés à des services juridiques, à la discrétion des assurés.
- Les consultants en intrusion informatique fournissent des conseils juridiques, notamment en répondant aux enquêtes réglementaires, en défendant les réclamations des contreparties et des personnes visées par les données touchées et en donnant des conseils sur les options de récupération.
- Les consultants en informatique mènent à bien les tâches de restauration, d'investigation et de clôture.
- Tout autre sous-traitant conclut l'activité.
- Rapport final.
- Tout coût d'interruption des activités potentielle fait l'objet d'une évaluation et d'une préparation.

Communiquez avec notre équipe de souscripteurs spécialisés de Markel Cyber.

Nous nous adressons à un large éventail d'entreprises, tout en ayant la souplesse nécessaire pour examiner les cas les plus atypiques. Markel offre une variété de ressources et de services de gestion des risques à ses clients Cyber 360.

Notre équipe

Ed Rawe
Vice-président adjoint, Cyber
437-215-6881
Ed.Rawe@markel.com

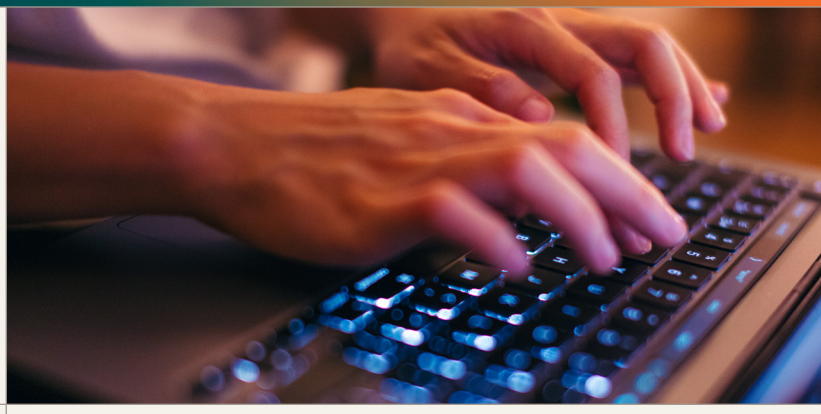
MARKEL

Fournisseurs de Markel Cyber 360 Canada

Markel s'associe à divers experts non exclusifs pour s'assurer que vous disposez des ressources dont vous avez besoin avant, pendant et après un cyberincident. Cette liste de fournisseurs partenaires de base n'est pas exhaustive; d'autres fournisseurs peuvent être engagés en fonction des besoins.

Si vous faites face à un incident de sécurité, notre service d'assistance téléphonique vous mettra en relation avec les services et les ressources nécessaires pour résoudre rapidement un événement assuré, 24 heures sur 24, 7 jours sur 7, 365 jours par année.

Veuillez communiquer avec : Norton Rose Fulbright S.E.N.C.R.L, s.r.l.
1-866 -BREACHX / 1-866-273-2249
nrfc.breach@nortonrosefulbright.com



Services de consultants en intrusion informatique

Avocats spécialisés dans les événements liés à la cybersécurité et à la protection des renseignements personnels. L'avocat aide à interpréter les réglementations de l'État ainsi que les responsabilités en vertu de la loi, à rédiger des lettres de notification aux clients et à assurer la coordination avec les experts en la matière.

Norton Rose Fulbright S.E.N.C.R.L, s.r.l.

Entreprises de restauration des données

Entreprises spécialisées dans la récupération post-cyberattaque, offrant des services qui permettent aux organisations de rétablir rapidement leurs activités et leurs données.

Arctic Wolf

Fenix24

Criminalistique et restauration

Des experts tiers qui aident à l'enquête et à la restauration.

Mandiant

Kroll

Crowdstrike

Arctic Wolf

Négociations de rançons

Des négociateurs experts tiers, qui ont une connaissance approfondie des acteurs de la menace et qui ont l'habitude d'obtenir des résultats favorables.

One Arrow

Cyber Steward

Fournisseurs de Markel Cyber 360 Canada

Communications en situation de crise

Des spécialistes de la réponse aux crises qui proposent des communications stratégiques pour sauvegarder et renforcer votre réputation.

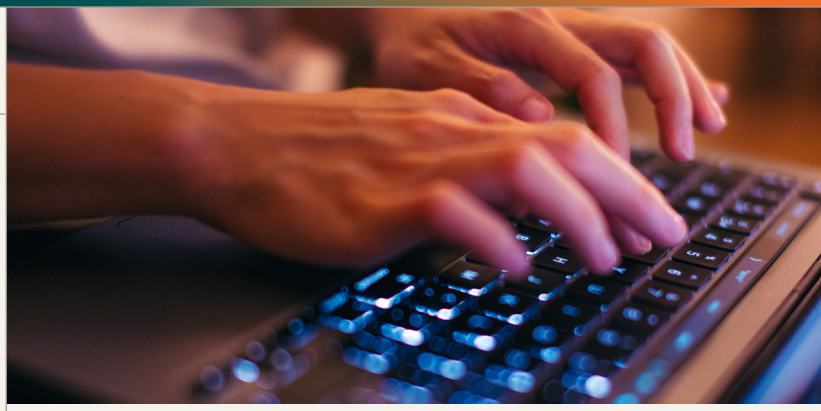
Navigator

Surveillance du crédit, notification et restauration de l'identité

Services de surveillance du crédit pour les personnes dont les données personnelles ont pu être compromises.

Equifax

Transunion



Expertise comptable judiciaire

Les experts-comptables judiciaires évaluent et quantifient les dommages pécuniaires afin d'assurer la transparence financière et de garantir l'exactitude des demandes d'indemnisation.

Baker Tilly

Gestion des risques

Services préventifs vous préparant aux scénarios potentiels, complétés par des outils concrets visant à diminuer la fréquence et la gravité des cyberincidents.

Black Kite

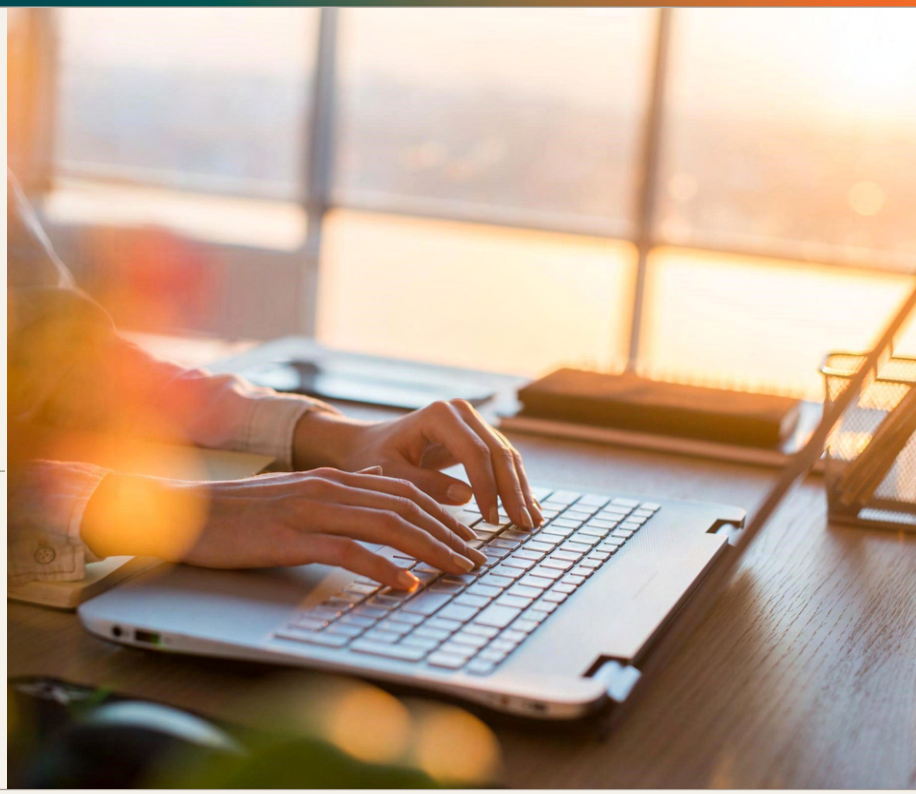
Norton Rose Fulbright S.E.N.C.R.L., s.r.l.

Markel Cyber 360 Canada
Services de prévention de l'atteinte à la sécurité des données Guardian 360

Tous les clients qui souscrivent Cyber 360 peuvent bénéficier d'un appel d'accueil relatif aux réclamations pour en savoir plus sur la manière dont nos partenaires spécialisés dans l'intervention en cas d'atteintes à la sécurité peuvent vous aider en cas de cyberincident. Dans le cadre de cette assistance, les clients auront également accès à la plateforme de Black Kite l'un des principaux fournisseurs de renseignements sur les cyberrisques tiers —, qui propose une évaluation non invasive par balayage de ports afin d'aider les organisations à mieux comprendre et à gérer leurs risques en matière de cybersécurité.

Markel Cyber 360 Canada est conçu pour soutenir votre entreprise à chaque étape d'un cyberincident — avant, pendant et après —, vous permettant ainsi de garder une longueur d'avance.

En réponse à la demande croissante de protection proactive, les assurés admissibles peuvent également recevoir l'accès à l'une des offres Guardian 360 ci-dessous, en plus de l'appel d'accueil préalable à une atteinte à la sécurité des données et de l'accès à Black Kite. Chaque produit Guardian 360 comprend un menu de services en cybersécurité et en protection de la vie privée soigneusement sélectionnés, et les assurés peuvent sélectionner un service privilégié à activer dans le cadre de leur garantie.



Guardian 360 Core

Les partenaires spécialisés en matière d'atteinte à la sécurité des données peuvent fournir des mises à jour sur la protection de la vie privée, la cybersécurité et l'intelligence artificielle ou une première consultation sur les cyberrisques ou un service d'examendes contrats, conformément à ce qui est décrit ci-dessous :

1. Des bulletins d'information hebdomadaires sur la protection de la vie privée, ainsi qu'un accès exclusif à des tables rondes trimestrielles axées sur la protection de la vie privée, la cybersécurité et l'intelligence artificielle, réunissant des pairs et des experts du secteur pour obtenir des connaissances actuelle.
2. Un examen de haut niveau de vos politiques et procédures actuelles de gouvernance en matière de cybersécurité, des discussions stratégiques sur les obligations prévues aux lois et aux règlement et identification des domaines à haut risque immédiat.
3. Un examen d'un maximum de deux contrats importants comprenant des informations sur les risques potentiels.

Guardian 360 Plus

Les partenaires spécialisés en matière d'atteinte à la sécurité des données peuvent fournir des évaluations des cyberrisques, des exercices de simulation sur table ou des examens de contrats, notamment :

1. La réalisation d'une évaluation des cyberrisques, d'un examen d'un plan d'intervention en cas d'incidents existant, ou l'aide à l'élaboration d'un tel plan, et l'identification des lacunes en matière de conformité aux principales réglementations.
2. Un exercice virtuel de simulation sur table avec les principales parties prenantes d'une durée d'une heure.
3. Une liste de contrôle personnalisée répertoriant les réglementations fédérales et provinciales pertinentes en matière de cybersécurité.
4. Un examen d'un maximum de cinq contrats importants comprenant des informations sur les risques potentiels.

Services Markel Cyber 360 Canada

Guardian 360 Pro

Les partenaires spécialisés en matière d'atteinte à la sécurité des données peuvent fournir un examen complet de politiques, un exercice de simulation sur table personnalisé, une liste de contrôle de la conformité à la réglementation ou un examen des contrats, conformément à ce qui est décrit ci-dessous :

1. Un examen complet d'un maximum de deux politiques clés — comme en matière d'intervention en cas d'incidents ou de conservation des données —, comprenant des recommandations d'experts pour se conformer aux exigences légales et aux pratiques exemplaires du secteur.
2. Un exercice virtuel de simulation sur table d'une durée de deux heures, adapté à un secteur d'activité et à un profil de risque particuliers, suivi d'une séance de compte rendu et de rétroaction afin de renforcer la préparation.
3. Une liste de contrôle personnalisée précisant les réglementations fédérales et provinciales applicables en matière de cybersécurité.
4. Un examen d'un maximum de cinq contrats importants, offrant un aperçu des risques potentiels et des améliorations de clauses recommandées pour soutenir la conformité et la résilience.

Guardian 360 Ultra

Les partenaires spécialisés en matière d'atteinte à la sécurité des données peuvent fournir une évaluation complète de la préparation face aux cyberincidents, la rédaction d'un plan d'intervention en cas d'incident, des exercices de simulation sur table personnalisés, des analyses des lacunes en ce qui concerne la conformité à la réglementation, une formation offerte au conseil d'administration ou à la direction ou des conseils en matière de gestion des fournisseurs, conformément à ce qui est décrit ci-dessous :

1. Un examen complet de l'ensemble des politiques, procédures et contrats relatifs à la cybersécurité et des entretiens avec le personnel clé afin d'évaluer l'état de préparation.
2. Un exercice immersif sur table d'une durée de trois heures comprenant des scénarios réels, une rétroaction en direct et une prise de décisions stratégiques comprenant un résumé détaillé des leçons tirées, des enseignements clés et un plan d'action des éléments à améliorer en priorité.
3. Un examen de la conformité réglementaire : une analyse des lacunes en ce qui concerne votre conformité aux lois et aux règlements applicables en matière de cybersécurité réalisée par un expert.
4. Une formation sur les cyberrisques destinée aux équipes dirigeantes : une formation personnalisée destinée aux cadres ou aux membres du conseil d'administration, comprenant les obligations légales et les études de cas réels.
5. Des conseils d'experts en matière de gestion des fournisseurs, y compris un modèle d'évaluation des risques et des clauses relatives à la cybersécurité standard recommandées pour les contrats et les accords avec les fournisseurs afin d'assurer une résilience continue.