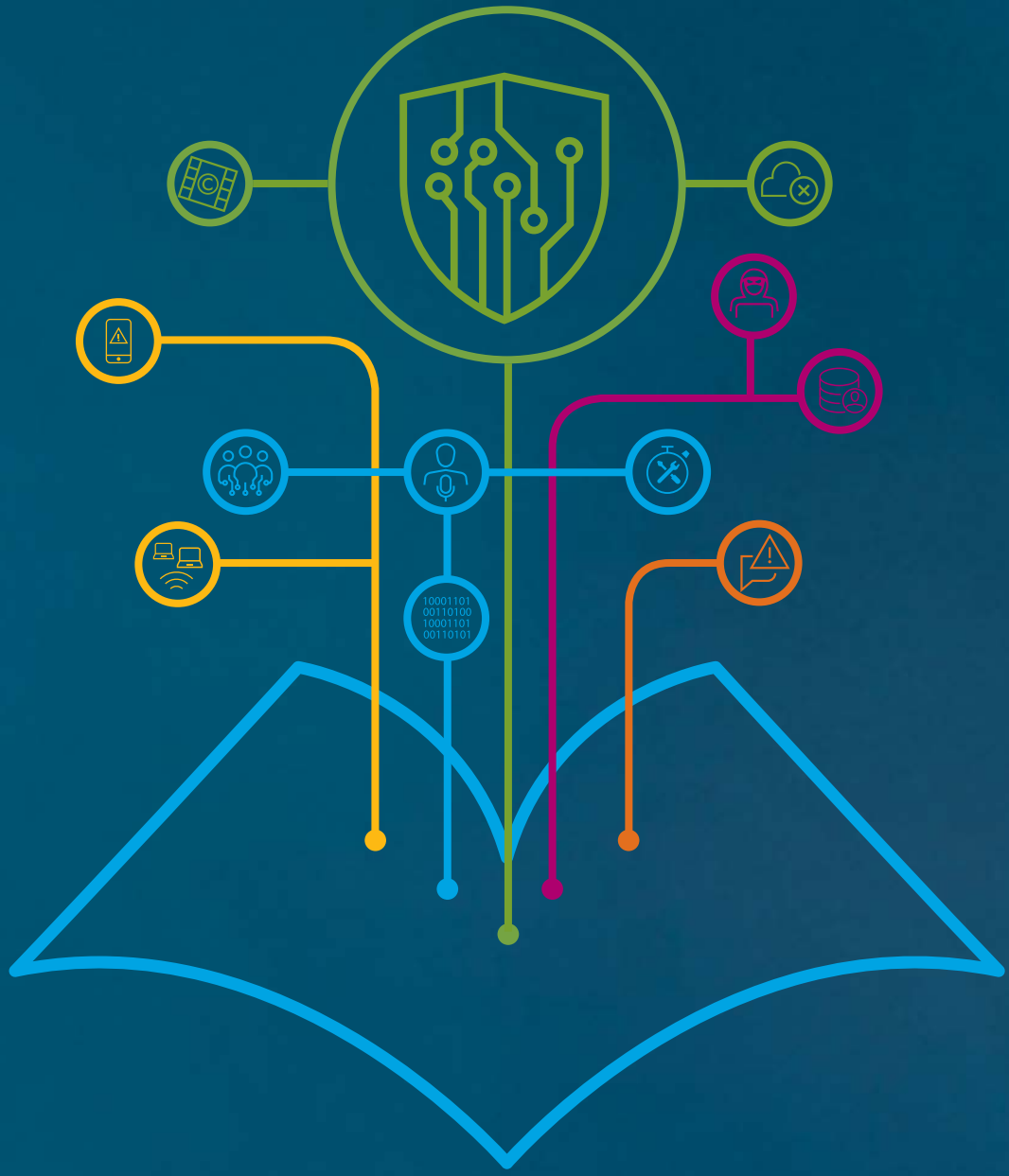
Tout savoir sur

CyberEdge®



AIG®

CyberEdge

La révolution numérique reste un axe de développement pour les entreprises, tant sur le plan opérationnel que commercial, tout en faisant naître de nouveaux enjeux complexes en matière de cybersécurité. Dans un monde en rapide évolution, CyberEdge fournit aux entreprises une solution complète de gestion des risques cyber.

Cette brochure vous présente certaines des garanties offertes par la police CyberEdge. Pour plus de précisions sur la nature et l'étendue de l'assurance CyberEdge, veuillez consulter les conditions générales et particulières de votre contrat ou consulter votre courtier.

Tout savoir sur CyberEdge :

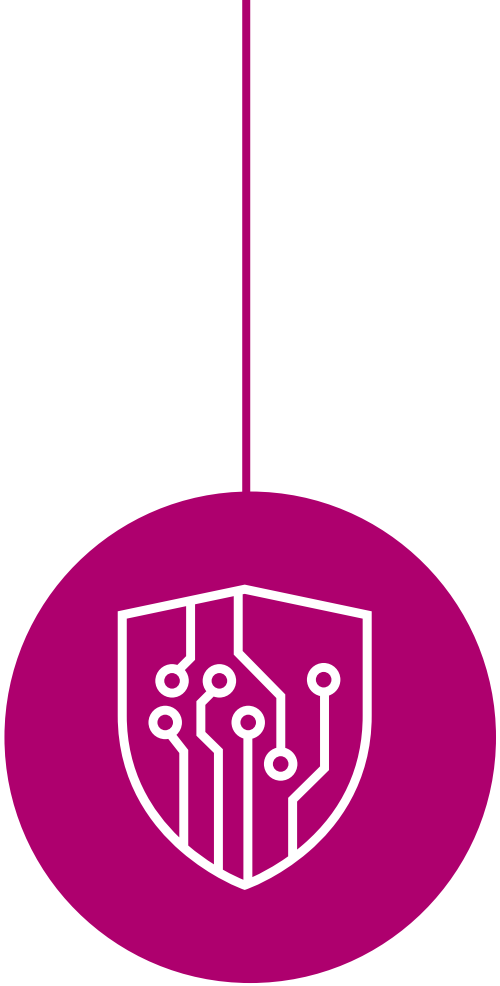
Garanties

Tout savoir sur CyberEdge :

Outils et services inclus dans l'offre CyberEdge

Tout savoir sur CyberEdge :

Services offerts par nos prestataires privilégiés



Tout savoir sur CyberEdge :

Garanties

Réseaux et données sont plus que jamais au cœur des activités des entreprises. En cas d'atteinte à la sécurité informatique, les pertes financières pour une société peuvent être très lourdes. CyberEdge est une police qui permet aux entreprises de se procurer une protection parfaitement adaptée à leurs besoins.

Voici quelques-unes des garanties proposées.

Actions d’urgence

Lorsqu’elles suspectent une attaque cyber, les entreprises ont rarement les moyens de diagnostiquer le problème et d’y répondre rapidement. La garantie Actions d’urgence de CyberEdge leur permet de contacter en urgence un consultant juridique et un expert informatique qui unissent leurs forces pour répondre aux besoins immédiats. Aucune franchise ne s’applique pendant la période initiale.

ZOOM

Dès qu’ils détectent un incident cyber, les clients ayant souscrit cette garantie peuvent appeler la ligne d’assistance CyberEdge pour organiser les premières mesures d’urgence.

Ils seront mis en contact avec un consultant juridique expérimenté (exerçant au sein d’un cabinet d’avocats de premier plan) dans un délai de deux heures. L’obtention de conseils juridiques le plus tôt possible joue un rôle clé pour la bonne coordination des interventions.

Si le problème est de nature technique, un expert informatique choisi parmi nos partenaires évaluera la situation et remédiera le plus rapidement possible aux failles de sécurité.

Il n’est pas rare que la menace provienne d’un problème de réseau sans gravité. Étant donné que cette garantie ne comporte pas de franchise, les clients ne seront pas pénalisés pour avoir consulté nos experts.

ZOOM :

Attaque Cyber et Réponses de CyberEdge

	VIOLATION DE LA SÉCURITÉ	EXPERTISE INFORMATIQUE	CONSEIL JURIDIQUE ET COMMUNICATION DE CRISE	NOTIFICATION	ENQUÊTE ET SANCTIONS ADMINISTRATIVES	RESPONSABILITÉS
Phases						
Réponse CyberEdge	Réponse et intervention d'un consultant juridique dans les deux heures qui suivent la notification de sinistre.	Expertise informatique : diagnostic, limitation, réparation ou restauration des données	Consultants juridiques et experts en communication de crise pour protéger la réputation de l'entreprise.	Coûts de notification des victimes potentielles et de surveillance des données volées afin de limiter les pertes.	Frais d'investigation préliminaire suite à une enquête administrative ou judiciaire et prise en charge des sanctions assurables imposées par les autorités réglementaires.	Frais de défense et dommages-intérêts dans les cas suivants : • atteinte aux données personnelles ou confidentielles • contamination des données de tiers par un virus • vol de codes d'accès à des systèmes • erreur ou négligence commise par un préposé

Gestion de Crise

Après une attaque cyber, une entreprise a besoin de différents services pour rétablir son activité. Le volet Gestion de crise de CyberEdge prend en charge les frais juridiques, informatiques et de relations publiques ainsi que les frais de monitoring et de surveillance, en complément des coûts de restauration des données et des frais de notification.

EXEMPLE DE SINISTRE :

Commerçants / Grande distribution - Atteinte à la sécurité des données

Près de trois millions de mots de passe ont été volés à un fournisseur de services en ligne et ont été divulgués sur Internet.

L'équipe de gestion des sinistres d'AIG et le consultant référent ont travaillé main dans la main avec l'assuré pour prendre les mesures qui s'imposaient : recommander aux personnes concernées de renouveler leurs mots de passe, prodiguer des conseils de sécurité aux utilisateurs, envoyer une communication par e-mail et donner les coordonnées de l'équipe d'assistance aux trois millions de clients potentiellement affectés.

Ce scénario de sinistre est fourni à titre d'illustration uniquement. L'étendue et les conditions d'application des garanties dépendent de chaque événement ou sinistre et sont assujetties aux dispositions de la police d'assurance.

ZOOM :

Règlement général sur la protection des données

Le Règlement général sur la protection des données entrera en vigueur en mai 2018. Les nouvelles dispositions établissent plus clairement les droits des personnes concernées et imposent davantage d'obligations aux entreprises qui traitent des données à caractère personnel.

L'un des éléments notables du nouveau règlement est la hausse du montant des amendes en cas de non-conformité. Les entreprises pourraient devoir payer jusqu'à 20 millions d'euros d'amende, ou 4 % de leur chiffre d'affaires annuel global. Par ailleurs, elles seront tenues de notifier aux autorités réglementaires toute violation, réelle ou alléguée, dans un délai de 72 heures.

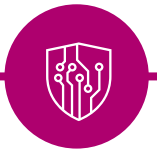
Le Règlement général fera de la protection des données une question relevant du conseil d'administration, quand ce n'est pas déjà le cas, et contraindra les entreprises à se pencher de près sur la réponse à apporter aux violations de la sécurité.

Responsabilité Civile

La garantie Responsabilité Civile couvre les réclamations de tiers faisant suite à une atteinte à la sécurité du système informatique. Sont pris en charge les frais de défense et les dommages-intérêts résultant d'une atteinte aux données personnelles et/ou confidentielles.

Enquêtes et Sanctions

La garantie Enquêtes et Sanctions couvre les frais de défense et les amendes assurables encourus lors d'une enquête d'une autorité administrative.



Pertes d'exploitation

Presque toutes les entreprises en contact avec les consommateurs s'appuient désormais largement sur le Web pour les ventes directes ou la gestion de la relation client. Même les secteurs traditionnels, comme la fabrication et les transports, ont besoin d'une connexion réseau pour fonctionner efficacement. La garantie Pertes d'exploitation couvre la perte de marges brutes et les dépenses engagées pour les atténuer en cas d'interruption ou de suspension d'activité suite à une atteinte à la sécurité du système informatique (frais supplémentaires d'exploitation).

EXEMPLE DE SINISTRE :

Commerçants / Grande distribution - Interruption de réseau

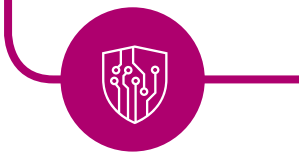
Un commerçant spécialisé dans la vente de vêtements à l'échelle nationale a subi une panne de système de 48 heures juste avant un week-end férié de grande activité, entraînant l'impossibilité de traiter les achats par carte de crédit, des pertes de clientèle et des perturbations dans la gestion des commandes.

AIG a choisi avec l'assuré un expert sinistre ayant pour mission de calculer la perte de chiffre d'affaires, qui a été évaluée à environ 1,4 million d'euros, après respect du délai de carence applicable tel que mentionné dans le tableau de garanties de la police.

Ce scénario de sinistre est fourni à titre d'illustration uniquement. L'étendue et les conditions d'application des garanties dépendent de chaque événement ou sinistre et sont assujetties aux dispositions de la police d'assurance.

Pertes d'exploitation : Prestataires externes

Les prestataires d'externalisation fournissent aux entreprises toute une série de services précieux comme l'hébergement en ligne, le traitement des paiements, la collecte et le stockage des données. La garantie Pertes d'exploitation couvre la perte de marge brute et les coûts d'atténuation résultant d'une faille de sécurité ou de système chez le prestataire.



Pertes d’exploitation : Défaillance

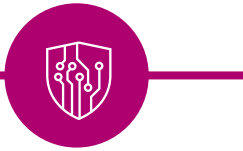
Toutes les défaillances des systèmes ne sont pas imputables à une atteinte à la sécurité. Une panne imprévue ou non intentionnelle peut également entraîner une interruption du réseau et des pertes d’exploitation. La garantie Pertes d’exploitation prévoit la couverture des pertes d’exploitation résultant d’une défaillance des systèmes internes non consécutive à un incident de cybersécurité.

Incident technique

Une attaque cyber n’est pas toujours la cause d’une perte ou d’un vol de données. Une surtension, une surchauffe, un événement naturel ou un acte de vandalisme peuvent également rendre les données inaccessibles. La garantie Gestion de crise prévoit la prise en charge des frais suite à un incident technique.

Média

L'environnement numérique évolue si rapidement que les entreprises peuvent, sans le vouloir, porter atteinte à des droits de propriété ou s'approprier du contenu créatif. La garantie Média couvre les frais de défense et les dommages-intérêts résultant d'une violation des droits de propriété intellectuelle ou d'une négligence vis-à-vis de tout contenu électronique.



ÉCLAIRAGE :

Exemple de cyberextorsion

Des hackers ont pénétré le réseau informatique de l'assuré et introduit le virus « Cryptolocker » dans son système. Ce logiciel malveillant a verrouillé le réseau de l'assuré et demandé une rançon de 3 000 € pour le rendre de nouveau accessible.

L'assuré a déclaré le sinistre à AIG et à la gendarmerie. Celle-ci lui a conseillé de ne pas payer la rançon et AIG lui a apporté son aide pour engager un expert informatique qui a effectué une analyse des systèmes et éradiqué le virus dans les 48 heures. L'expert informatique a découvert que le logiciel avait été téléchargé dans le système de l'assuré par le Directeur des Ressources Humaines qui avait été victime d'un hameçonnage (« phishing »). Les hackers avaient déguisé le virus en invitation WebEx et, en y répondant, le Directeur des Ressources Humaines a, sans le savoir, téléchargé le logiciel.

Pour détruire le virus et décrypter les données, l'assuré a réglé 50 000 € de frais d'expertise, qu'AIG lui a remboursés.

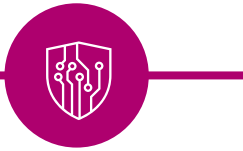
Ce scénario de sinistre est fourni à titre d'illustration uniquement. L'étendue et les conditions d'application des garanties dépendent de chaque événement ou sinistre et sont assujetties aux dispositions de la police d'assurance.

Cyber-extorsion

Les entreprises peuvent être la cible de cybercriminels qui se servent de logiciels malveillants pour prendre en otage leurs données et demander une rançon en échange de leur restitution. Le volet Cyber-Extorsion de CyberEdge couvre les frais résultant d'une menace d'extorsion. Sont compris les rançons exigées pour mettre fin au chantage ainsi que les frais engagés par des conseillers spécialisés en cyber-extorsion.

Fraude téléphonique

Appelée fraude d'accès au PBX (autocommutateur d'entreprise), cette attaque cible les systèmes téléphoniques pour passer des appels vers des numéros surtaxés. L'extension de garantie Fraude téléphonique de CyberEdge couvre le coût de surconsommation téléphonique résultant d'un accès et d'une utilisation non autorisés du système téléphonique d'une entreprise dans ses locaux professionnels.



Fraude informatique

L'escroquerie au transfert d'argent est une forme de criminalité informatique. Les hackers exploitent les informations obtenues suite à une faille de sécurité informatique pour transférer frauduleusement de l'argent depuis le compte d'un client tenu auprès d'un établissement financier. L'extension de garantie Fraude informatique de CyberEdge couvre les pertes financières directement engendrées par des transferts de fonds électroniques frauduleux résultant d'une faille de sécurité informatique.

Coupons

Les incidents cyber peuvent porter atteinte à la relation entre une entreprise et ses clients. Les compensations, telles que les rabais ou les remises, peuvent se révéler très efficaces pour corriger cette mauvaise impression. L'extension de garantie Coupons de CyberEdge permet de proposer à un client une compensation plutôt qu'une surveillance de ses données confidentielles.

Tout savoir sur CyberEdge :

Outils et services inclus dans l'offre CyberEdge

CyberEdge propose un ensemble de services de prévention qui contribuent à réduire les probabilités de survenance d'une attaque cyber et permettent aux entreprises d'améliorer la qualité de leur sécurité informatique.

Application mobile CyberEdge

Grâce à l'application mobile CyberEdge, les clients peuvent consulter les dernières actualités en matière de risques cyber, des opinions d'experts et des analyses de risques. Cette application est disponible sur iPhone, iPad, et Android™.

Scan de vulnérabilité des infrastructures*

Des experts réalisent à distance un audit de vulnérabilité des infrastructures web externes de l'entreprise, afin d'aider les clients à identifier les faiblesses susceptibles d'être exploitées par des hackers. Ce service permet d'identifier les risques cachés et les classe par ordre de priorité. Il fournit également aux entreprises un compte rendu détaillé des faiblesses identifiées, afin qu'elles puissent mieux évaluer, comprendre et rendre compte de leur niveau de sécurité.

Services de blocage proactif et formation*

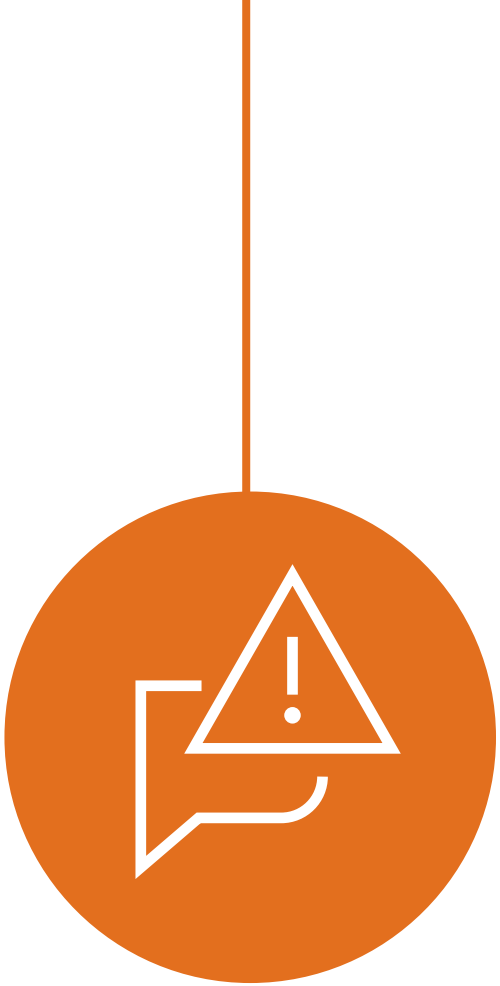
Avant une attaque, les hackers effectuent souvent une visite de reconnaissance afin de confirmer que l'adresse IP visée est une cible valable. Le dispositif de blocage appelé *shunning* les empêche d'atteindre le réseau. Le risque d'intrusion ultérieure s'en trouve fortement réduit. Si le réseau a déjà été attaqué, le système de blocage peut également bloquer les flux de données sortants à destination des serveurs des hackers, ce qui aura pour effet de désamorcer le logiciel malveillant. Une formation en ligne est également comprise dans l'offre. Il s'agit d'une mesure de prévention qui permet de réduire le principal risque cyber pour une entreprise : l'erreur humaine.

*Offerts gratuitement aux assurés d'une police CyberEdge pour toute prime supérieure à 5 000€. Services fournis par des tiers.

Portail d'informations sur la cybersécurité*

Le portail d'informations sur la cybersécurité est une plateforme centralisée d'informations techniques et éducatives sur la sécurité informatique. Il se révèle particulièrement utile pour la prévention des incidents cyber. Parmi les ressources disponibles, des conseils pour la formation des collaborateurs, des articles de fond et d'actualité sur l'environnement cybernétique et des systèmes d'évaluation des risques cyber.

* Offerts gratuitement aux assurés d'une police CyberEdge pour toute prime supérieure à 5 000 €. Services fournis par des tiers.



Tout savoir sur CyberEdge :

Services à des tarifs préférentiels

Forts de 20 ans d'expérience dans le domaine de la cybersécurité, nous avons soigneusement sélectionné des partenaires, experts en risques cyber, qui proposent aux assurés CyberEdge des services à des tarifs préférentiels.

Dark Net Intelligence

Par K2 Intelligence

K2 Intelligence travaille avec les assurés qui souhaitent connaître les dernières rumeurs qui circulent sur eux sur le dark net. K2 Intelligence arpente le dark net au moyen de moteurs de balayage électronique (appelés « web crawlers ») et d'autres outils sophistiqués de collecte de données pour permettre aux entreprises d'agir pro- activement face à la gestion des risques cyber.

Évaluation du niveau de maturité des systèmes de l'entreprise face à la cybersécurité

Par RSA

Tous les assurés CyberEdge bénéficient d'un abonnement de six mois à la solution de gestion de la Gouvernance, du Risque et de la Conformité (GRC) proposée par RSA, afin d'évaluer les risques liés à la cybersécurité. Cette solution se base sur le référentiel de cybersécurité du National Institute of Standards and Technology pour évaluer le niveau de cybersécurité d'une entreprise et l'aider à identifier des axes d'amélioration. C'est un outil conçu idéalement pour les grandes entreprises ou les réseaux d'infrastructures publiques (électricité, télécoms, santé publique).

Analyse de la vulnérabilité des entreprises

Par BitSight Technologies

BitSight évalue et contrôle les réseaux des entreprises et de leurs fournisseurs, et leur attribue une note en fonction de leur niveau de sécurité. BitSight opère sans perturber le travail des entreprises, en mesurant de manière continue les données disponibles depuis l'extérieur.

Analyse de la vulnérabilité des prestataires de services

Par Security Scorecard

Les entreprises tendent à ignorer les risques auxquels s'exposent les partenaires, les fournisseurs et les prestataires externes. L'analyse de vulnérabilité des prestataires permet d'évaluer et de contrôler la sécurité des réseaux de l'entreprise et de ses prestataires externes en leur attribuant une note. Nos clients peuvent ainsi garder un œil sur l'écosystème de leurs prestataires et identifier ceux qui sont les plus risqués. Nos spécialistes peuvent réaliser une démonstration sur demande.

Sensibilisation et Formation

Par Wombat Security

Formation des employés à la sécurité informatique, notamment aux techniques de phishing par le biais de simulations. Wombat utilise une méthode unique qui repose sur les quatre grands piliers d'un programme de sensibilisation et de formation à la cybersécurité : évaluer, éduquer, renforcer et contrôler. Nos spécialistes peuvent réaliser une démonstration sur demande.

SecureDNS

Par RiskAnalytics

SecureDNS fournit aux entreprises une protection permanente contre les menaces inhérentes aux serveurs DNS en identifiant les communications provenant de domaines malveillants et en redirigeant les utilisateurs vers une page de renvoi sûre ou les commandes malveillantes vers un « gouffre » DNS. Cette technologie supprime l'un des moyens les plus couramment utilisés par les hackers pour tromper les utilisateurs ou les hameçonner, pour introduire des logiciels de rançon ou des virus dans les systèmes, supprimer des données volées ou lancer une attaque cyber.

Analyse de portefeuille

Par AXIO

Les assurés CyberEdge peuvent faire appel à Axio Global (Axio) pour obtenir une vision globale des risques cyber auxquels ils sont exposés et harmoniser plus efficacement leurs contrôles technologiques et opérationnels et leur couverture d'assurance. La méthode élaborée par Axio couvre l'ensemble des risques cyber, y compris les risques de vol de données, de mise en jeu de la responsabilité, de dommages matériels, de dommages environnementaux, de dommages corporels et de perturbation de l'activité.

ÉCLAIRAGE :

Expertise en gestion des sinistres dans le monde entier

Chez AIG, nous traitons environ quatre sinistres informatiques par jour. Nos équipes de souscription et de gestion des sinistres travaillent main dans la main pour offrir à nos clients une expérience inégalée.

aig.com/fr

FL00002432 1017 - FRDMC 001. CE. 03.2021