PACK Cyber
Brochure sinistres

Les situations relatées dans ce document ont été établies sur la base des sinistres déclarés ou réglés par AIG. Ces exemples ont été volontairement simplifiés pour en faciliter la lecture et pour préserver l'identité de leurs protagonistes.

Les décisions d'indemnisation relatées dans les exemples fournis sont communiquées à titre indicatif et n'ont aucune valeur contractuelle. Elles ne peuvent en aucun cas être opposées à AIG ou préjuger de décisions futures de AIG concernant l'indemnisation de sinistres survenus dans des circonstances similaires.

>> Cyber-extorsion : Rançongiciel / ransomware

① Une PME a reçu un email de l'un de ses fournisseurs réclamant le règlement urgent d'une facture. Il s'agit en réalité d'un faux message, et la pièce jointe est un ransomware / logiciel-rançon qui crypte un grand nombre de données du système informatique de l'entreprise, rendant ces dernières totalement inaccessibles. Le pirate informatique réclame une rançon de 800 € pour débloquer les données.

La PME appelle la cellule de crise. Le coordinateur de la cellule l'oriente vers un expert, afin qu'il puisse analyser le problème et déterminer si le cryptage peut être ou non facilement défait.

AIG a pris e en charge les frais de l'expert, le montant de la rançon, les frais de reconstitution des données ainsi que la perte d'exploitation subie par l'entreprise pendant la durée du blocage de son activité pour un montant de 60 000 €.

② Une association reçoit un email de l'un des EHPAD qu'elle gère lui communiquant des informations financières à regarder d'urgence. Il s'agit d'un faux message et la pièce jointe est en réalité un logiciel malveillant qui crypte un grand nombre de données du système informatique de l'association, rendant ces dernières totalement inaccessibles. Le hacker réclame une rançon de 10 000 € pour débloquer les données.

Des mesures d'urgence sont mises en œuvre :

- Intervention d'un expert informatique, pendant 72h, afin de décrypter les données et solutionner l'incident.
- Intervention d'un expert en communication de crise afin de mettre en place un plan de communication et d'éviter au maximum les risques d'image pour l'association.

AIG a pris en charge les frais de reconstitution des données pour un montant de 45 000€.

La réglementation européenne visant à obliger la notification auprès des personnes ayant vu leurs données personnelles diffusées (« GRDP » applicable depuis le 25 mai 2018) a engendré un coût de 100 000 €, pris en charge par le contrat d'assurance Cyber.

③ Une société, proposant notamment la réalisation de solutions de télécoms, reçoit un mail de l'un de ses prestataires lui communiquant une facture suite à une intervention chez un client. Il demande bien évidemment un règlement rapide.

Il s'agit en fait d'un faux message et la pièce jointe est en réalité un logiciel malveillant qui crypte un grand nombre de données du système informatique de la société, rendant ces dernières totalement inaccessibles.

Le pirate informatique réclame une rançon de 1 Bitcoin (monnaie virtuelle ayant un cours qui évolue quotidiennement) soit 2 400 € pour débloquer les données.

Les données de la société (les données personnelles des salariés) ainsi que les données de ses clients sont cryptées.

Le consultant informatique, partenaire d'AIG, solutionne l'incident. Le consultant en communication de crise aide la société à rédiger un communiqué de presse afin d'éviter au maximum des risques d'image.

Les garanties enclenchées sont : Mesures d'urgence et gestion de crise. L'assureur a pris en charge l'ensemble des frais pour un montant de 37 000 €.

>> Attaque par déni de service (Distributed Danial of Service DDoS)

Le site Internet de réservation d'une franchise de location de véhicules est rendu inaccessible. Plus aucune réservation ne peut être effectuée.

Des mesures d'urgence sont mises en œuvre :

- Intervention d'un expert informatique, pendant 72h sans franchise, afin de déterminer la méthode d'attaque, d'émettre des recommandations et de remettre en marche et sécuriser le service.
- Intervention d'un expert en communication de crise afin de mettre en place un plan de communication en cas de besoin.

AIG a pris en charge les réclamations au titre de la responsabilité civile et la perte d'exploitation pour un montant de 28 000 €.

>> Vols / pertes de données

① Un hacker s'est introduit dans le système informatique d'une société et a réussi à modifier l'un des fichiers exécutés lors de la connexion au compte client. Cette modification a permis au hacker de recevoir le nom d'utilisation (adresse email) et le mot de passe des clients de l'entreprise.

Cette intrusion a été détectée lors d'une maintenance de routine.

Les clients de l'assuré, du fait de cette intrusion, sont en risque lorsqu'ils utilisent ce même couple adresse/mot de passe sur des sites plus sensibles comme par exemple leur messagerie électronique, leur compte Paypal…

PACK Cyber
Brochure sinistres

Suite à l'appel de l'assuré à la cellule de crise, AIG a pu accompagner rapidement l'assuré en mettant à sa disposition un consultant informatique pour déterminer la méthode d'attaque et émettre des recommandations.

Il a été accompagné par un consultant en communication afin de prévenir les 6 500 clients impactés.

La nouvelle réglementation européenne visant à obliger la notification auprès des personnes ayant vu leurs données personnelles diffusées (« GRDP » applicable au 25 mai 2018) a engendré un coût de 400 000 €, pris en charge par le contrat d'assurance Cyber.

② Une intrusion malveillante dans les serveurs de sauvegarde d'une société spécialisée dans la téléphonie et les câblages réseaux a permis le vol de données (personnelles et confidentielles) de ses clients.

Suite à l'appel de l'assuré à la cellule de crise, AIG a pu accompagner rapidement l'assuré en mettant à sa disposition un consultant informatique pour solutionner le litige ainsi qu'un consultant en communication de crise afin de préparer les communications adéquates pour limiter les risques d'image.

Les garanties déclenchées dans cette situation : mesures d'urgence et gestion de crise. AIG a pris en charge 35 000 € de frais pour ce sinistre.

La réglementation européenne visant à obliger la notification auprès des personnes ayant vu leurs données personnelles diffusées (« GRDP » applicable depuis le 25 mai 2018) a engendré un coût de 170 000 €, pris en charge par le contrat d'assurance Cyber.

③ L'ancien Responsable des Services Informatiques (RSI) d'une société dans l'édition de logiciel et l'infogérance, après avoir été licencié, s'est introduit dans le système informatique de la société et a reformaté les disques durs. Cette attaque a engendré une perte massive de données.

L'assuré a été dirigé vers un expert informatique, qui a trouvé la faille. Avant son départ, le RSI avait dissimulé une borne wifi qui lui permettait de s'introduire dans le système informatique de la société.

L'expert information a procédé à la fermeture de cette borne wifi et à la récupération des données.

En parallèle, le consultant en communication, qui lui a été recommandé par l'assureur, a rédigé un communiqué à l'attention des clients de la société.

Grâce à l'intervention de ces experts, l'assuré a pu éviter une perte d'exploitation supplémentaire, des réclamations de tiers et diminuer les effets sur sa réputation et son image. Le coût pris en charge par AIG est d'environ 80 000€.

La réglementation européenne visant à obliger la notification auprès des personnes ayant vu leurs données personnelles diffusées (« GRDP » applicable depuis le 25 mai 2018) a engendré un coût de 140 000€, pris en charge par le contrat d'assurance Cyber.

PACK Cyber
Brochure sinistres

④ Un sous-traitant dans le domaine aéronautique reçoit une alerte de source anonyme signalant une faille de son système informatique ayant entraîné une fuite de données confidentielles de ses fournisseurs.

Les données figurent sur un site « miroir » accessible depuis Google, avec des éléments confidentiels, les codes sources, les plans de vol…

Suite à l'appel de l'assuré à la cellule de crise, AIG a déployé les consultants nécessaires à la résolution de cette attaque :

- L'expert informatique :
  - détermine la méthode d'attaque, identifie la faille. La fuite est imputable à une erreur interne.
  - évalue les données atteintes
  - effectue les démarches auprès de Google pour assurer la disparition définitive du site miroir et des données.

- Le conseil en communication de crise :
  - assiste à la rédaction de la lettre pour les fournisseurs impactés
  - met en place un plan de communication si demandes presse

- Le cabinet d'avocats :
  - coordonne les différents intervenants
  - émet ses premiers conseils juridiques afin de limiter l'impact du sinistre
  - rédige la lettre d'information aux fournisseurs impactés

Le coût pris en charge par AIG est d'environ 80 000 €.

NOTA: Ces illustrations de sinistres sont spécialement rédigées de manière générale dans un but informatif et n'ont pas pour objet d'être une représentation factuelle et exacte de situations réelles garanties ou non par le contrat d'assurance. L'étendue et les conditions d'application des garanties sont soumises aux dispositions du contrat d'assurance. L'application des garanties est sujette au processus de gestion de sinistre, spécifique à chaque circonstance et situation particulière. Le contenu de ce document et ses descriptions ne peuvent pas être opposés pour justifier l'application d'une garantie.