



Cyber-protection totale d'HSB^{MC}

Cyberassurance complète pour les petites et moyennes entreprises

HSB Canada, membre de Munich Re, est une entreprise axée sur la technologie, fondée sur l'assurance spécialisée et l'ingénierie, qui s'efforce de stimuler l'innovation dans un monde moderne afin que vous puissiez demeurer à l'avant-garde des risques.

Les cybercriminels utilisent une multitude de méthodes d'attaque et de nouvelles menaces émergent constamment. La Cyber-protection totale d'HSB, un programme complet de cyberassurance, est conçue pour fournir une protection contre un large éventail de cyberrisques, créée sur mesure pour les petites et moyennes entreprises.

Tout le monde est à risque

Les cybercriminels peuvent de toute évidence s'introduire dans le système informatique de n'importe quelle organisation, des grandes entreprises aux agences d'évaluation du crédit. Si de grandes entreprises sophistiquées dotées de cyberrisques robustes peuvent être infiltrées, quelles sont les chances des petites et moyennes entreprises de subir un tel sort?

Les petites et moyennes entreprises canadiennes sont vulnérables aux cyberattaques

21 pour cent des petites entreprises et 65 pour cent des moyennes entreprises ont subi une cyberattaque dans le passé. Plus de la moitié des PME pensent qu'il est possible qu'elles soient actuellement vulnérables à une cyberattaque ou à une violation de données, en particulier si elles sont plus grandes qu'une entreprise à propriétaire unique. Les PME qui vendent également des produits ou des services en ligne sont deux fois plus susceptibles de penser qu'elles sont vulnérables que celles qui vendent uniquement en magasin.*

Si cela leur est arrivé, n'importe qui peut en être victime

Pratiquement toutes les petites et moyennes entreprises sont à risque, parce qu'elles disposent d'ordinateurs

et d'appareils portables, stockent des données, conservent les renseignements personnels d'individus et dépendent d'Internet. De plus, les cyberrisques ne se limitent pas aux attaques électroniques. Un employé pourrait perdre un ordinateur portable ou une clé USB, ou envoyer un courriel contenant des données personnelles à une mauvaise adresse par inadvertance. Aussi, de nombreuses violations se produisent lorsque des dossiers physiques contenant des informations sensibles sont supprimés ou lorsqu'un vieil ordinateur est jeté.

Coût du cyberrisque

Le coût des événements de cyberrisques est considérable. Parmi les petites et moyennes entreprises qui ont été attaquées, 58 pour cent ont déclaré que cela leur avait coûté moins de 100 000 \$, et 41 pour cent qu'elles avaient déboursé au moins 100 000 \$.*



Lorsqu'un cyberévénement se produit, les entreprises sont confrontées à plusieurs problèmes. La confusion et le chaos règnent, alors que l'entreprise cherche à comprendre ce qui s'est passé et comment y répondre. Un incident doit faire l'objet d'une enquête par un spécialiste judiciaire des TI; un

conseiller juridique est souvent nécessaire; et les notifications aux clients doivent être envoyées rapidement. Les victimes de cyberattaques affirmeront que la portion la plus longue et la plus coûteuse de l'événement concerne la récupération et la reconstitution des données. De plus, les entreprises interrompent généralement leurs systèmes dès qu'elles sont informées d'un cyberévénement, les empêchant de poursuivre leurs activités, entraînant une perte de revenu.

Éléments essentiels de la Cyber-protection totale d'HSB

La Cyber-protection totale d'HSB offre un ensemble de huit garanties fournissant une protection d'assurance multiniveaux contre les cyberrisques complexes et en constante évolution.

- **Frais d'intervention contre la compromission des données** – Paie les assurés pour l'évaluation judiciaire des TI, la notification des violations, les services d'alerte de fraude et de gestion de cas, les conseillers juridiques, les services de relations publiques, les amendes et les pénalités imposées par des organismes de réglementation et dans l'industrie des cartes de paiement (PCI) à l'égard de la sécurité des données.
- **Cyberassurance complète contre les attaques informatiques des petites et moyennes entreprises** – Paie les frais de restauration et de reconstitution des données ainsi que de restauration des systèmes en raison d'une attaque informatique endommageant les données et les logiciels; y compris les pertes d'exploitation et les services de relations publiques.
- **Cyberextorsion** – Couvre les frais et les paiements du négociateur ou

de l'enquêteur des assurés afin d'éliminer une menace de rançongiciel ou d'extorsion.

- **Responsabilité pour la compromission des données** – Couverture de tierce partie pour des actions en justice par des personnes touchées ou des jugements intentés par des entités fédérales ou réglementaires.
- **Responsabilité pour la sécurité du réseau** – Couvre les coûts de règlement et de défense des assurés pour les poursuites alléguant la négligence d'un assuré à l'égard de la sécurité informatique.
- **Responsabilité pour les médias électroniques** – Couvre les coûts de règlement et de défense engagés par les assurés dans une action en justice alléguant une violation de droit d'auteur ou de marque de commerce, une diffamation à l'égard d'une personne ou d'une organisation, ou une atteinte du droit à la vie privée d'une personne.
- **Récupération de l'identité** – Services de récupération de l'identité pour les propriétaires d'entreprise; la gestion de cas et le remboursement des dépenses pour les frais innommés divers, les frais juridiques, les salaires perdus ainsi que les frais de soins d'enfants et de personnes âgées.
- **Fraude liée aux paiements détournés** – Paie les pertes financières directes résultant d'une tromperie criminelle au moyen de communications par courrier électronique, télécopie ou téléphone pour inciter un assuré, ou une institution financière auprès de laquelle un assuré a un compte, à envoyer ou à détourner de l'argent, des titres ou des biens corporels.

Admissibilité

La plupart des classes d'affaires sont admissibles à la Cyber-protection totale d'HSB et aucune proposition distincte n'est exigée. Pour des classes sélectionnées, certaines options de limites requièrent un questionnaire afin de déterminer l'admissibilité à ces limites.

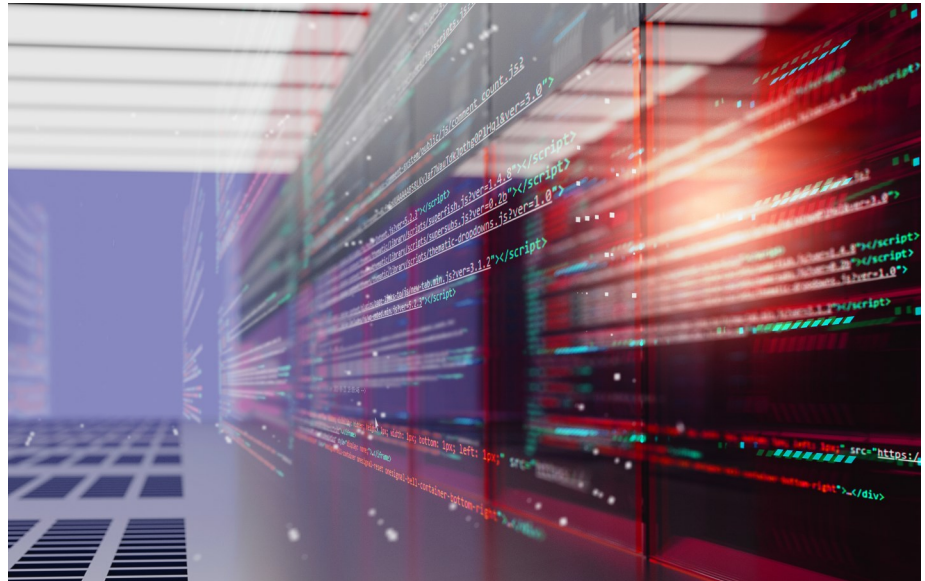
- Classes limitées : entreprises de traitement de données, compagnies de sous-traitance informatique, établissements d'enseignement (y compris écoles privées/publiques, collèges et universités), municipalités.
- Classes non admissibles : institutions financières, établissements réservés aux adultes, maisons de jeu/casinos, entreprises de traitement de cartes de crédit ou de transactions financières, hôpitaux, agences d'évaluation du crédit, agents de recouvrement, courtiers en information/données.

Limites

La Cyber-protection totale d'HSB est assujettie à une limite globale, les options varient de 25 000 \$ à 1 000 000 \$. Des sous-limites peuvent s'appliquer pour certaines garanties.

Franchises

Les franchises de la Cyber-protection totale d'HSB varient de 1 000 \$ à 10 000 \$ par événement, selon l'option de limite sélectionnée.



Réponse de la Cyber-protection totale d'HSB

Le service de cyberréclamation d'HSB est distinct. Certains fournisseurs représentant des assureurs étrangers dégroupent le processus de réclamation et abdiquent les décisions aux avocats qui paient simplement les factures. Nous procédons différemment.

Les cyberexperts en sinistres d'HSB sont des spécialistes qualifiés pour aider les assurés à se rétablir de l'événement. Nos cyberexperts en sinistres agissent en tant que gestionnaires, encadrant les assurés et coordonnant l'intervention de plusieurs fournisseurs afin d'aider les titulaires de police à accélérer le processus de reprise des activités et ainsi réduire les incidences. Un peu comme un « cyberange » pour les assurés, ils fournissent des conseils et mobilisent les ressources spécialisées pour l'évaluation judiciaire des TI, les

conseils juridiques, les services de notification, la restauration de systèmes, les relations publiques et autres dont les assurés ont besoin pour se rétablir.