EgR STRATÈGES EN ASSURANCE

Présentation Assurance Cyber – Novembre 2021

LACUNES DES POLICES D'ASSURANCE TRADITIONNELLES

CES LACUNES PEUVENT COMPRENDRE :

1. L’absence de couverture en vertu d’une police de responsabilité civile générale, parce qu’un événement lié à la cybersécurité ne correspond pas aux définitions des déclencheurs de la couverture;

2. L’absence de couverture en vertu d’une police d’assurance « tous risques », parce que la perte entraînée par une atteinte à la cybersécurité ne constitue pas une perte de biens tangibles;

3. La compréhension des distinctions entre une police d’assurance contre le crime et une police d’assurance de cybersécurité, ainsi que de leur complémentarité.

****ATTENTION: EXLCUSION CONTRE LES RISQUES CYBER****

SOMMAIRE ASSURANCE CYBER

À la base – police monoligne:

Intervention en cas d'incident

- Coach d'intervention
- Services juridiques
- Information judiciaire
- Notification
- Surveillance du crédit
- Relations publiques

Dommages Directs

- Extortion
- Pertes de revenus
- Rétablissement des données

Responsabilité

- Responsabilité liée à la protection de la vie privée
  +Réglementation + cartes de paiement
- Responsabilité liée à la confidentialité
- Responsabilité des médias

TENDANCES DE MARCHÉ

1. Fréquence et sévérité des réclamations à la hausse
    a. Complexité des scénarios de brèches = frais de gestions de crise à la hausse
2. Connaissances des scénarios de réclamation
    a. Meilleures connaissances des scénarios de pertes par les assureurs = prévisibilité et impact sur les couvertures offertes
    b. Environnement réglementaire davantage punitif
3. Réduction de capacité, diminution de limites et ajouts d’exclusions
4. Processus de souscription exhaustif, tant pour les renouvellements que les nouvelles affaires
5. Correction importante dans la tarification

PROCESSUS DE SOUSCRIPTION - 8 ÉLÉMENTS DE CYBER SÉCURITÉ QUI SONT ANALYSÉS PAR LES DIFFÉRENTS ASSUREURS

1. Authentification multi-facteur pour la connexion à distance et l'accès aux courriels
2. Technologie de détection et de réponse aux menaces envers les ordinateurs et serveurs
3. Plan de relance des affaires qui comprend le volet Cyber
4. Gestion active du réseau informatique et des applications
5. Monitoring des réseaux contre les intrusions
6. Procédure formelle relative à la mise à jour des applications et implantation des patchs
7. Appliquer les procédures de contrôles relatives aux paiements
8. Gestion des exposés qui proviennent de fournisseurs de service tiers

RÉCLAMATIONS – SCÉNARIOS VÉCUS ET MÉDIATISÉS

1. Manufacturier de produit de béton – Attaque informatique qui a paralyse les machines de production – Frais de gestion de l'incident: 250,000$

2. Distributeur de machinerie – Attaque par ransomware, suivi d'un incident en Ingénierie sociale – Perte liée à l'ingénierie sociale: 120,000$

3. Distributeur d'équipement électrique – Accès non-autorisé aux données de l'entreprises, et fuite de ces données – Frais de gestion comprennent la notification aux individus, gestion de crédit et 2 semaines de travail par l'équipe TI pour remise à niveau du réseau (i.e. perte de revenus)

5
BUREAUX
au Québec en mesure de répondre à vos besoins internationaux

75
ANNÉES
d'expertise

PLUS DE
150
PROFESSIONNELS
à votre service

1 SEULE MISSION | CONTRIBUER AU SUCCÈS DES ENTREPRISES D'ICI

EgR