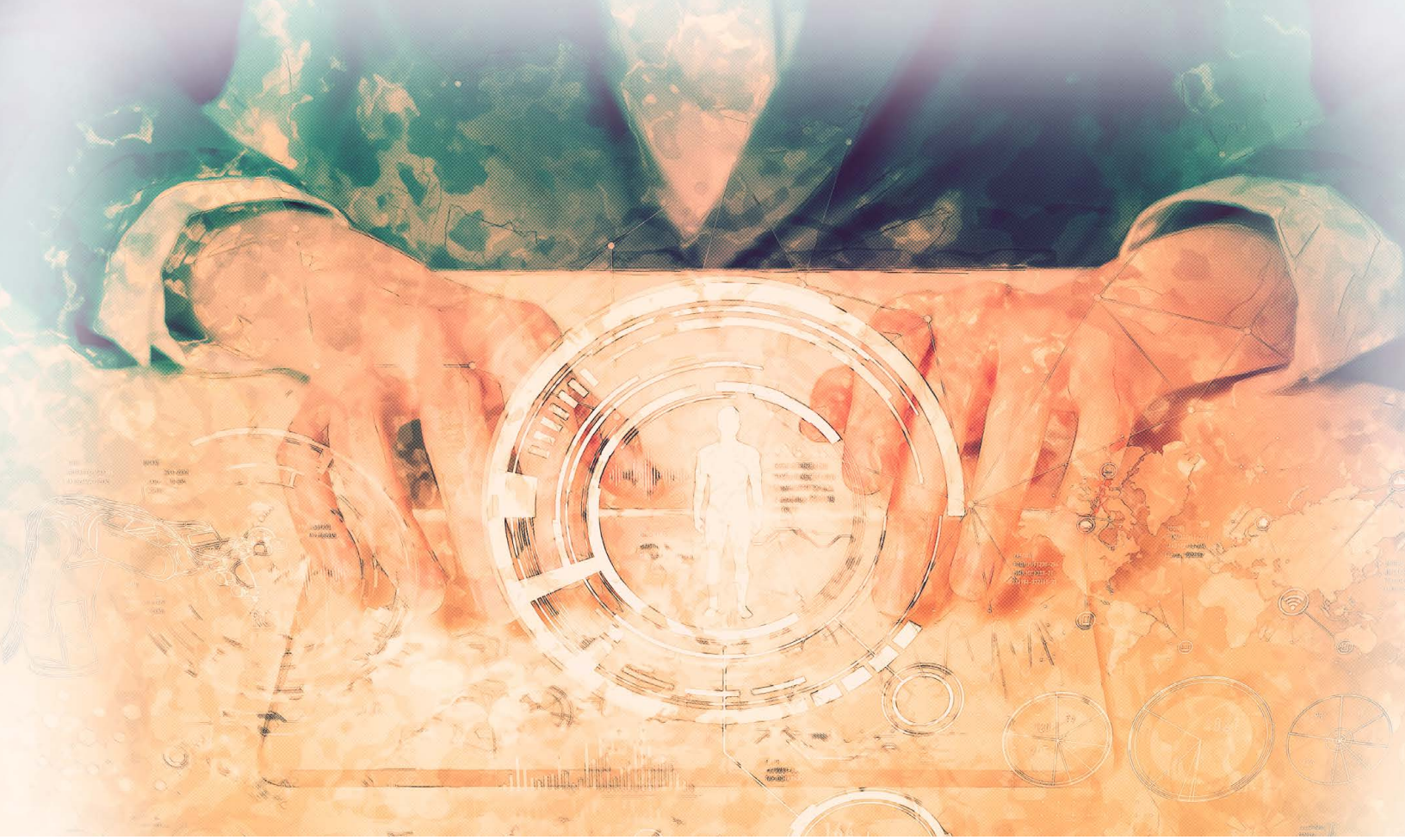
L'ASSURANCE DES CYBERRISQUES :

Démêler le vrai du faux

CYBERSCOUT® | Northbridge™ Assurance

Il circule des tas d'idées fausses au sujet des atteintes à la protection des données, de la protection des renseignements personnels et de l'assurance des cyberrisques. En fait, les institutions financières sont peut-être même aussi mêlées que leurs clients, ce qui peut mettre les entreprises en danger. Après tout, si vous croyez ne pas avoir besoin d'une certaine assurance, ou si vous pensez être protégé alors que vous ne l'êtes pas, un cyberévénement pourrait se révéler désastreux pour votre entreprise.

La solution? Mieux connaître les différents types d'assurance des cyberrisques et se faire conseiller sur la protection qui convient le mieux aux besoins uniques de son entreprise. Les institutions financières familiarisées avec les plus récents programmes sont peut-être les mieux placées pour évaluer les options dont disposent leurs clients, et les clients bien avisés peuvent s'assurer que toutes les facettes de leur entreprise ont été prises en compte. Une fois que vous aurez lu le présent document technique, vous aurez toute l'information dont vous avez besoin pour collaborer avec un fournisseur d'assurance et choisir l'assurance des cyberrisques qui pourrait sauver votre entreprise en temps de crise.



L’évolution de l’assurance des cyberrisques

Détrompez-vous : la cybercriminalité n’est pas un phénomène récent, même qu’elle existe depuis un bon bout de temps – tout comme l’assurance des cyberrisques. Depuis l’arrivée des premières solutions d’assurance au début des années 90, à l’époque où la technologie commençait à prendre plus de place dans le quotidien et où Internet devenait un outil commercial viable, les premières assurances couvrant les interruptions de service et la responsabilité civile liée aux sites Web ont donné naissance à une panoplie de solutions contre le vol d’identité et les atteintes à la protection des données. **Mais est-ce que ces solutions ont suffisamment évolué pour être à la hauteur des risques d’aujourd’hui?**

Le chemin parcouru

Au fur et à mesure de l’évolution des sites Web, qui sont passés du pendant numérique des panneaux d’affichage à des plateformes d’affaires dynamiques, l’interconnectivité a explosé. Des programmes axés sur la responsabilité civile liée aux réseaux informatiques ont vite emboîté le pas, et ont gagné en popularité auprès des plus grandes sociétés et des entreprises en ligne spécialisées.

L'ampleur des risques auxquels font face les entreprises d'aujourd'hui a poussé les institutions financières à créer un vaste éventail de solutions de services de gestion des vols d'identité et des atteintes à la protection des données. Ces solutions ont été conçues non seulement pour résoudre les problèmes propres au commerce électronique, mais aussi pour contrer les risques relatifs aux atteintes à la protection des données des clients et à l'interruption des activités en ligne, ainsi que les nouvelles cybermenaces comme les rançongiciels et la cyberextorsion.

Même si les entreprises ont désormais plus d'options, l'assurance des cyberrisques n'est pas aussi répandue qu'elle le devrait. En effet, plusieurs compagnies d'assurance n'offrent pas ce type d'assurance, et celles qui le font proposent des solutions différentes, ce qui complique la tâche aux clients au moment de comparer les différentes polices d'assurance.

Les prochaines étapes

Malgré toute l'attention médiatique accordée aux plus importantes atteintes à la protection des données, certaines idées fausses, voire une certaine indifférence, restent ancrées dans la tête des propriétaires d'entreprise : beaucoup croient qu'ils n'ont pas besoin de se protéger contre les cyberrisques comme les atteintes, ou que leur assurance générale actuelle couvre déjà ces risques. Ils ne s'embêtent donc pas à souscrire une assurance des cyberrisques pour leur entreprise. Malgré tout, de plus en plus d'atteintes graves font la manchette, ce qui alimente la peur à l'égard des cyberrisques et incite les gens à agir.

Vous ne savez pas par où commencer? Vous n'êtes pas le seul : plusieurs de vos semblables sont dans le même bateau, car il est parfois difficile de bien comprendre la portée et l'étendue des différentes polices d'assurance des cyberrisques offertes sur le marché. Les entreprises de services financiers peuvent grandement vous aider à choisir et à développer le programme contre les cyberrisques le mieux adapté à votre entreprise en tirant parti de leurs vastes connaissances des cyberrisques qui vous guettent actuellement.

Comprendre les risques pour connaître ses options

La compréhension des risques, et de la meilleure façon de les atténuer, est au cœur d'une protection proactive. Vous êtes peut-être bien outillé pour améliorer votre posture de sécurité et réduire votre risque d'être victime d'une atteinte, mais pour déterminer et mettre en œuvre des mesures efficaces, vous devrez mieux connaître les cybermenaces actuelles et la capacité de votre entreprise à y faire face.

Le passage des programmes étroitement ciblés à des programmes multirisques polyvalents a entraîné une certaine confusion. Déterminer les risques auxquels votre entreprise est exposée et trouver la meilleure façon de les atténuer n'est plus aussi facile qu'il y a cinq ans, mais des conseils d'experts sur les pratiques exemplaires du moment peuvent vous aider à associer chaque risque à la bonne stratégie d'atténuation.

Vous ne savez pas par où commencer? Vous n'êtes pas le seul : plusieurs de vos semblables sont dans le même bateau, car il est parfois difficile de bien comprendre la portée et l'étendue des différentes polices d'assurance des cyberrisques offertes sur le marché.

À chaque programme son utilité

La première étape, et l'une des plus importantes, consiste à connaître les programmes de protection numérique les plus courants – et ce qui les distingue.

Voici quelques explications sur les caractéristiques propres à chaque programme :

1. Programmes de cybersécurité

Ces programmes sont axés sur les services et les systèmes technologiques, et l'usage qu'en fait l'entreprise. Les risques couverts comprennent ceux relatifs à la conception de sites Web et de logiciels, à l'équipement de réseau, aux dommages causés par les interruptions de service et les virus, ainsi qu'à la majorité des services fournis par les fournisseurs de technologie et les consultants.

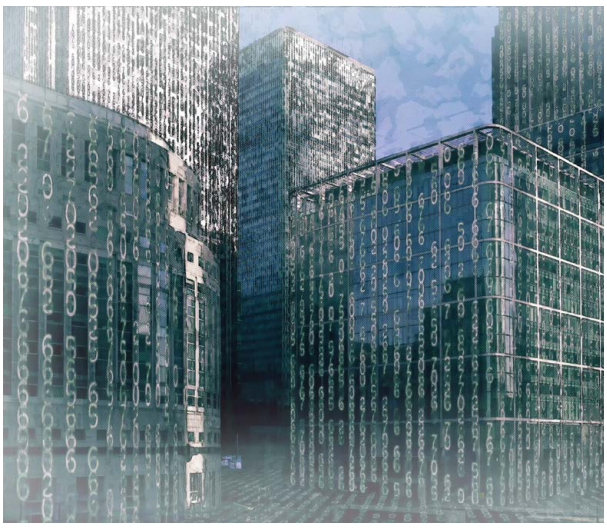
En règle générale, les clients sont aussi couverts pour les dommages causés par un virus qu'ils transmettent par inadvertance à un réseau appartenant à autrui ou exploité par un tiers.

2. Programmes liés aux atteintes à la protection des données

Ces programmes sont souvent appelés « programmes de protection des renseignements personnels » ou « programmes de protection contre les atteintes à la sécurité ». Ils protègent les entreprises en cas de compromission ou de divulgation de données de nature délicate. La plupart des polices de ce type couvrent également les frais relatifs à l'intervention de l'assuré et à la responsabilité civile envers les tiers.

3. Programmes liés à la protection des renseignements personnels

Plus généraux, les programmes liés à la protection des renseignements personnels peuvent protéger les entreprises si les données d'un client, d'un consommateur ou d'un patient venaient à être compromises ou divulguées.



Les programmes liés à la protection des renseignements personnels protègent les entreprises en cas de compromission ou de divulgation de données de nature délicate.

Comprendre les différences entre les protections

Lorsqu'il est question des polices d'assurance offertes, les termes « protection contre les cyberrisques » et « protection contre les atteintes à la confidentialité » sont souvent utilisés de façon interchangeable, même s'ils sont très différents l'un de l'autre.

Protection contre les cyberrisques :

Ce type de protection couvre généralement les services et les systèmes technologiques, et l'usage qu'en fait l'entreprise.

Les risques couverts comprennent ceux relatifs à la conception de sites Web et de logiciels, à l'équipement de réseau, aux dommages causés par les interruptions de service et les virus, ainsi qu'à la majorité des services fournis par les fournisseurs de technologie et les consultants. De plus, les entreprises sont généralement couvertes pour les dommages causés par un virus qu'elles transmettent par inadvertance à un réseau appartenant à autrui ou exploité par un tiers.

Protection contre les atteintes à la confidentialité :

Cette protection couvre les entreprises en cas de compromission ou de divulgation des données d'un client,

d'un consommateur ou d'un patient. Ces polices d'assurance couvrent parfois aussi les frais relatifs à l'intervention de l'assuré et à la responsabilité civile envers les tiers.

Garanties visant les pertes subies par l'assuré :

Ce type de garantie couvre les dépenses engagées en vertu d'exigences réglementaires, comme des mandats fédéraux et des règlements régissant l'industrie financière, mais aussi d'ententes contractuelles en matière de conformité.

Les dépenses engagées pour faire enquête afin de déterminer la portée et la durée de l'incident, quelles données ont été compromises et quelles personnes ont été touchées sont aussi couvertes, tout comme les frais engagés pour répondre à une atteinte, en aviser les personnes concernées et les organismes de réglementation pertinents, et fournir aux victimes (et aux victimes potentielles) des services de surveillance du crédit et de rétablissement à la suite d'un vol d'identité.

Garanties visant les pertes subies par un tiers :

Ce type de garantie couvre les frais de défense engagés dans le cadre de litiges ou d'actions réglementaires découlant d'une atteinte.

Une protection contre les cybercrimes ou contre les cyberrisques

Les notions de cybercrime et de cyberrisque vous semblent peut-être similaires, mais elles relèvent en fait de deux catégories d'assurance distinctes. En effet, les cybercrimes sont couverts par l'assurance contre le vol, alors que les cyberrisques sont une catégorie à part entière.

Pensons notamment au piratage psychologique, qui désigne le fait de duper et de manipuler une personne afin qu'elle fasse certains gestes ou révèle de l'information de nature délicate. Si le piratage psychologique engendre des pertes financières, il est considéré comme un cybercrime. En revanche, s'il entraîne la divulgation de données confidentielles, il s'agit d'un cyberrisque.

Selon un récent sondage FICO, 40 % des entreprises canadiennes ont mis en place un programme de cybersécurité complet, c'est-à-dire qui couvre tous les risques possibles, alors que 50 % des entreprises interrogées des secteurs du commerce de détail et du commerce électronique pensent que leur protection actuelle ne correspond pas à leur profil de risque. Comment ces entreprises peuvent-elles remédier à la situation? Elles doivent d'abord évaluer leur niveau de risque selon leur propre profil.

40 % des entreprises canadiennes ont mis en place un programme de cybersécurité complet, c'est-à-dire qui couvre tous les risques possibles, alors que 50 % des entreprises interrogées des secteurs du commerce de détail et du commerce électronique pensent que leur protection actuelle ne correspond pas à leur profil de risque.

La taille et le secteur d'activité : les deux facteurs déterminants du risque relatif

Votre entreprise est-elle petite, moyenne ou grande? Lorsqu'il est question de cyberrisques, la taille est importante, car le volume de données traitées et votre approche quant à leur stockage peuvent vous exposer à certains risques.

Les grandes entreprises

En raison de la nature de leurs activités, les grandes entreprises ont habituellement besoin d'une protection solide contre les atteintes à la protection des renseignements personnels et les cyberrisques. En effet, comme elles recueillent, traitent et stockent généralement une grande quantité d'information, et qu'elles disposent souvent d'infrastructures de technologie et de réseautique complexes pour soutenir leurs activités, les grandes entreprises ont plus de sources de vulnérabilité que les autres – et ont souvent plus à perdre.

Souvent, ces entreprises déploient et gèrent l'essentiel des éléments fondamentaux qui sous-tendent un champ d'activités plus large, comme le traitement des transactions financières ou la compilation et l'analyse de vastes bases de données. Ces activités nécessitent de nombreuses liaisons avec des partenaires

externes, notamment des fournisseurs et des entreprises clientes, ce qui élargit le bassin de victimes potentielles. De plus, comme elles ont souvent recours aux services de fournisseurs externes, plusieurs grandes entreprises donnent accès à leur réseau à des personnes qui ne font pas partie de leur propre effectif, multipliant ainsi les risques d'être victime d'une atteinte.

Ces facteurs exposent les grandes entreprises à de grands risques de cyberincidents. Toutefois, les risques liés aux atteintes à la protection des renseignements personnels sont souvent circonscrits par la mise en place de politiques et de mesures de sécurité rigoureuses, que les grandes entreprises peuvent s'offrir en raison de leurs importants moyens financiers et de leurs vastes ressources internes.

Les petites entreprises

À l'opposé, beaucoup de petites et moyennes entreprises ne sont pas autant exposées aux cyberrisques que leurs grandes sœurs. Elles utilisent principalement leurs propres systèmes internes tout en collaborant à l'occasion avec d'autres entreprises afin de mettre en commun leurs réseaux dans le cadre d'activités menées en tandem.

Si les petites entreprises ne font généralement pas face aux mêmes cyberrisques que les grandes entreprises, elles sont plus susceptibles d'être victimes d'atteintes à la protection des renseignements personnels. Comme la plupart d'entre elles n'ont pas d'experts en protection des renseignements personnels ou de grandes équipes technologiques, les données qu'elles recueillent et traitent sont parfois plus vulnérables.

En outre, les petites entreprises ont moins tendance à mettre en place des politiques de conservation des données strictes, et ne connaissent peut-être pas les façons les plus sécuritaires d'entreposer et de détruire l'information. Dans bien des cas, les risques d'atteinte qui ne sont pas d'origine numérique inquiètent davantage les petites et moyennes entreprises. Par exemple, l'envoi de factures papier ou de relevés d'un patient à la mauvaise personne ou la destruction inadéquate de documents papier désuets peuvent entraîner des risques d'atteinte aussi graves que ceux posés par l'intrusion dans un réseau informatique.

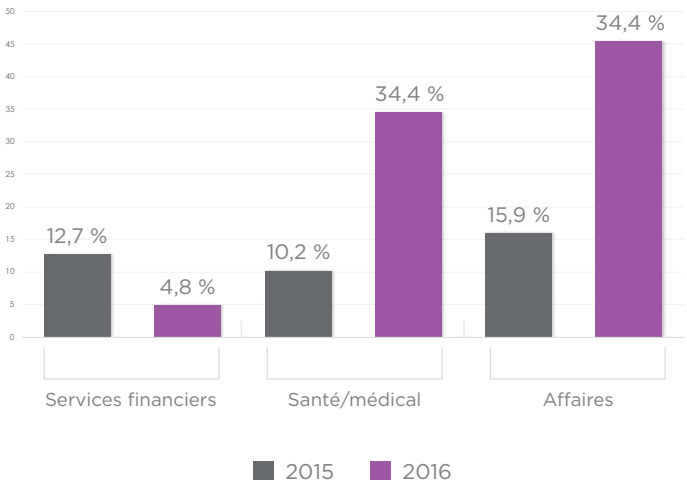
D'autres facteurs à prendre en considération

Le profil de risque de certaines entreprises, grandes ou petites, ne dépend pas que de leur taille. En effet, les entreprises évoluant dans certains secteurs particuliers, comme les soins de santé ou les services juridiques ou financiers, peuvent avoir besoin d'adopter des programmes plus robustes en matière d'atteinte à la protection des renseignements personnels.

Ces entreprises doivent traiter des données de nature particulièrement délicate qui, si elles étaient divulguées, pourraient causer un grave préjudice aux personnes concernées. Qu'il s'agisse d'un grand hôpital ou d'une petite clinique, d'un cabinet d'avocats national ou d'un avocat indépendant dans une petite ville, ces entreprises ont entre les mains des renseignements hautement confidentiels qui attirent les pirates, et dont elles doivent assurer la protection coûte que coûte.

Une analyse des atteintes survenues au cours d'une période récente de dix ans révèle certaines tendances sectorielles :

NOMBRE D'ATTEINTES PAR SECTEUR (2005-2016)



Ces données montrent que les secteurs des services financiers et du crédit arrivent mieux à contrer ces risques qu'auparavant, mais que ceux des services médicaux et des affaires connaissent une augmentation inquiétante du nombre d'atteintes.

Source : Données sur les atteintes du ITRC (2005-2016)

Une cyberstratégie solide pour votre entreprise

Bien que les besoins en matière de protection contre les cyberrisques et les atteintes à la protection des renseignements personnels varient en fonction de la taille de l'entreprise, d'autres facteurs de risque pourraient aussi dicter le choix du programme le mieux adapté à l'entreprise.

Les grandes entreprises comptent généralement plusieurs autres produits à valeur ajoutée dans leur portefeuille, et les programmes liés aux cyberrisques peuvent être un complément naturel aux initiatives supervisées par l'équipe de gestion des risques de l'entreprise. Il est aussi probable que ces équipes internes aient déjà trouvé d'où proviennent les faiblesses potentielles et la marche à suivre pour les corriger. Si les grandes entreprises assument régulièrement d'importants risques financiers, la plupart acceptent aussi le fait que des primes d'assurance élevées font partie du coût normal des affaires.

On pense souvent que les petites entreprises ne souhaitent pas adopter des programmes de sécurité robustes, ou qu'elles n'en sont pas capables, mais en réalité, plusieurs d'entre elles (surtout celles évoluant dans les secteurs à haut risque) gagneraient à souscrire une police d'assurance hautement ciblée et choisie avec soin. Souvent, l'ajout de garanties complémentaires peut venir renforcer une police d'assurance des entreprises déjà en place, mais ne peut enrayer tous les dangers : sans une assurance des cyberrisques complète, votre entreprise est-elle réellement protégée contre tous les cyberrisques?

Voici comment nous pouvons vous aider

Puisque les cyberrisques peuvent revêtir de nombreuses formes, il est essentiel que vous connaissiez votre exposition relative pour pouvoir élaborer un mécanisme de défense robuste. Bien qu'il soit important de protéger votre entreprise autant que possible, la bonne assurance pourrait venir à votre rescousse si vos efforts s'avéraient insuffisants.

Les assurances des cyberrisques ne sont pas toutes pareilles. Sans une assurance adaptée à votre situation, vous pourriez devoir assumer les frais juridiques, les amendes, les coûts de réparation et les frais de reprise des activités résultant d'une cyberattaque. De plus, les logiciels nuisibles comme les rançongiciels étant devenus plus complexes et généralisés, une seule attaque du genre pourrait vous causer d'importants problèmes financiers.

En partenariat avec CyberScout, Northbridge Assurance a mis au point l'Assurance des cyberrisques, un produit d'assurance polyvalent. En plus de protéger vos finances en cas de fuite de données, votre police vous donne accès à un assortiment complet de cyberressources, à une aide réactive et à des conseils personnalisés pour veiller à ce que ce genre d'incident ne se reproduise jamais. Après tout, la gestion des risques s'exerce en continu, et Northbridge prend cette gestion très au sérieux, notamment en vous offrant des polices complètes qui placent la réussite à long terme de votre entreprise au centre des priorités.

Northbridge Assurance | CYBERSCOUT®