LA COVID-19 ENTRAÎNE DES RISQUES DE CYBERSÉCURITÉ

La pandémie mondiale a forcé des millions d'employés à travailler à la maison avec relativement peu de formation ou de préparation pour ceux qui n'ont pas l'habitude de le faire. L'état actuel des choses augmente les risques de cybersécurité pour les entreprises de toute taille. Vous trouverez ci-dessous certains défis et des mesures suggérées pour minimiser les risques.

Perte de données et atteintes à la vie privée
Le travail à distance augmente la probabilité que :

- les appareils contenant des données de l'entreprise soient perdus ou volés (p. ex., ordinateurs portables ou appareils laissés dans les taxis ou d'autres endroits publics, des clés USB égarées)

- les employés utilisent des ordinateurs ou des appareils qui sont moins bien protégés que ceux utilisés au bureau ou qui fonctionnent tout à fait indépendamment des mesures de cybersécurité de l'entreprise (p. ex., pare-feu, antivirus, contrôle d'accès de connexion)

- les employés se fient à des réseaux Wi-Fi non protégés dans des endroits publics (p. ex., cafés, bibliothèques publiques) qui sont plus susceptibles d'être la cible d'attaques que les connexions sécurisées du bureau

Ces facteurs augmentent la probabilité de perte de données d'entreprise et d'atteintes à la vie privée en raison de fuites dans les renseignements confidentiels au sujet des employés et des clients.

Assurez-vous que vos employés connaissent les politiques de l'entreprise régissant l'utilisation et la sécurité des appareils. Si vous n'avez pas de telles politiques, c'est l'occasion d'envisager la mise en place de telles politiques.

Augmentation de la vulnérabilité aux cyberattaques
Les cybercriminels et les pirates informatiques utilisent la curiosité et la peur des gens contre eux par des attaques visant les utilisateurs à la recherche d'information sur la COVID-19 (p. ex., certains pirates envoient des courriels d'hameçonnage prétendant provenir d'organisations médicales ou de santé ou même des responsables de l'Organisation mondiale de la santé, alors que d'autres pirates affichent en ligne des cartes du virus infestées par des logiciels malveillants pour recueillir les renseignements personnels des utilisateurs).

La prolifération de telles attaques augmente la probabilité que certaines atteignent leur but. Rappelez à vos employés leur formation sur la sécurité de l'information et le danger de cliquer sur des courriels non sollicités. Si vous n'avez pas mis en place des formations obligatoires régulières sur la sécurité de l'information pour vos employés, vous devriez le faire aussitôt que possible.

Relâchement des contrôles financiers
Avoir plus de cadres qui travaillent à distance signifie qu'il peut être plus difficile de mettre en place les contrôles financiers existants pour prévenir la fraude (p. ex., il est plus difficile de recueillir les signatures pour approuver les transactions, lorsque les cadres ne sont pas au bureau ou sont difficilement joignables par téléphone, il est plus difficile de faire des rencontres en personne et des appels pour s'assurer que les consignes envoyées par courriel ne sont pas fausses). Les entreprises devraient surveiller les transactions de près et s'assurer que les solutions de rechange pour leur approbation permettent toujours l'authentification appropriée des consignes.

En ce qui concerne l'avenir
La crise mettra à l'épreuve la position des entreprises canadiennes en matière de sécurité et, pour plusieurs, la leçon sera dure et coûteuse. Si vous découvrez une atteinte à la sécurité, suivez votre plan de réponse aux incidents. Si vous avez une assurance cybersécurité, communiquez immédiatement avec votre conseiller en atteinte à la sécurité. Si vous n'avez pas d'assurance cybersécurité, vous devriez immédiatement appeler votre avocat et demander à un conseiller en sécurité de coordonner votre réponse et vos efforts de relèvement. Chaque heure, chaque jour compte lorsqu'il s'agit de répondre à une atteinte à la sécurité des données.
Si vous avez des questions au sujet de votre couverture d'assurance cybersécurité actuelle ou si vous désirez consulter un courtier pour déterminer la solution d'assurance cybersécurité qui répond à vos besoins professionnels ou à ceux de votre entreprise, communiquez avec BMS.

Brent J. Arnold, partenaire, Gowling WLG