LA COVID-19 AUGEMENTE LES RISQUES EN MATIERE DE CYBERSÉCURITÉ

Dans le sillage de la pandémie mondiale, des millions d'employés se sont vus obligés de travailler à domicile, alors que beaucoup d'entre eux n'en ont pas l'habitude, n'ont jamais suivi de formation adéquate et ont été peu préparés à cet égard. La situation actuelle accroît des risques en matière de cybersécurité pour les entreprises de toutes tailles. Nous presentons ci-dessous certaines des problématiques qui surviennent et les mesures suggérées pour minimiser les risques.

Perte de données et atteintes à la vie privée

Le travail à distance augmente la probabilité que :

- des appareils contenant des données d'entreprise soient perdus ou volés (p. ex., ordinateurs portables ou appareils oubliés dans un taxi ou un lieu public; clés USB égarées);
- les employés utilisent des ordinateurs ou des appareils dotés de protections inférieures à celles dont sont munis les équipements de bureau, ou qui fonctionnent entièrement en dehors du cadre des mesures de cybersécurité de l'entreprise (p. ex., pare-feux, protection contre les virus, contrôles d'accès aux ouvertures de session);
- les employés utilisent des connexions sans fil non sécurisées dans des espaces publics (cafés, bibliothèques publiques, etc.) qui sont plus susceptibles d'être attaquées que les connexions sécurisées dans les bureaux.

Ces facteurs augmentent la probabilité de perte de données d'entreprise et de violation de la vie privée en raison de la fuite de renseignements privés appartenant aux employés et aux clients.

Assurez-vous que vos employés connaissent les politiques de l'entreprise portant sur l'utilisation et la sécurité des appareils. Si de telles politiques n'existent pas au sein de votre entreprise, il s'agit d'un bon moment pour vous pencher sur la question et agir en conséquence.

Vulnérabilité accrue aux cyberattaques

Les cybercriminels et les pirates informatiques amateurs profitent de la curiosité et de l'anxiété des gens en lançant des attaques ciblant les utilisateurs à la recherche d'information sur la COVID-19 (p. ex., certains pirates informatiques envoient des courriels d'hameçonnage en se faisant passer pour une organisation sanitaire ou médicale, ou même pour des représentants de l'Organisation mondiale de la santé; d'autres mettent en ligne des cartes de régions touchées par le virus, lesquelles sont infectées par des logiciels malveillants, en vue de recueillir les renseignements personnels des utilisateurs).

La prolifération de ces attaques augmente la probabilité que certaines d'entre elles atteignent leurs cibles. Rappelez aux employés leur formation en matière de sécurité de l'information et le danger de cliquer sur des courriels non sollicités. Si vous n'avez pas déjà mis en place une formation régulière obligatoire sur la sécurité de l'information à l'intention des employés, tâchez de le faire dès que possible.

Relâchement des contrôles financiers

Puisque davantage de cadres travaillent à distance, il peut être plus difficile d'appliquer les mesures de contrôle financier habituelles en vue de prévenir la fraude (p. ex., il devient plus difficile d'obtenir des signatures d'approbation de transactions; les réunions en personne ou les appels pour vérifier que les instructions reçues par courrier électronique ne sont pas fausses deviennent plus compliqués lorsque les cadres ne sont pas au bureau ou facilement joignables par téléphone). Les entreprises doivent surveiller les transactions de près et en ce qui concerne l'obtention des approbations requises, s'assurer que l'application de solutions de rechange permette tout de même d'établir l'authenticité des instructions reçues.

Prévisions et mesures à prendre

Cette crise mettra à l'épreuve la position des entreprises canadiennes sur le plan de la cybersécurité et, pour beaucoup d'entre elles, les leçons seront dures et coûteuses. Si vous découvrez une faille de cybersécurité, suivez votre plan d'intervention en cas d'incident. Si vous avez une cyberassurance, contactez immédiatement votre coach désigné en cas de violation. Si vous n'avez pas de cyberassurance, nous recommandons d'appeler vos avocats immédiatement et de demander qu'un coach désigné en cas de violation coordonne votre intervention et vos mesures de rétablissement de la situation. Chaque heure et chaque jour comptent lorsqu'il s'agit de répondre à une violation de données.