Les mesures que les entreprises peuvent adopter pour protéger leurs secrets professionnels pendant la crise du COVID-19

11.05.2020 6 minutes de lecture

Auteurs

Antonella Carminatti

Le premier pas pour les entreprises est d'établir une politique de télétravail qui prenne en compte la nécessité de protection des secrets professionnels, ou de réévaluer les politiques existantes qui concernent cette nécessité. Même si beaucoup d'entreprises opèrent déjà dans le monde, les défis suscités par le transfert brutal de forces de travail entières vers le télétravail sont significatifs et sans précédents. Prévues pour des circonstances normales, les politiques de télétravail préexistantes ne sont probablement pas responsables des risques et défis provoqués par la crise du COVID-19. Même si ces politiques doivent respecter divers intérêts en concurrence, les entreprises doivent employer les protocoles suivants pour protéger leurs secrets professionnels et autres informations confidentielles.

1. Distribuer, Rappeler, Répéter

Distribuer régulièrement des rappels et des bulletins de confidentialité incitant les destinataires à la vigilance pendant le télétravail. Inclure dans ces rappels et bulletins, les informations de contact d'une (ou plusieurs) personne(s) désignée(s) qui répondra constamment aux questions et aux inquiétudes de ceux qui travaillent à la maison sur des secrets professionnels de l'entreprise et autres informations confidentielles

2. Limiter ou interdire l'utilisation de dispositifs ou comptes personnels dans les affaires de l'entreprise

Insister sur les interdictions et/ou limitations de l'utilisation de dispositifs personnels par les employés pour conduire les affaires de l'entreprise, particulièrement pour ce qui concerne les communications qui ont trait ou se réfèrent à des informations de secret professionnel. Même si des employés, contractuels ou fournisseurs, ont accès et sauvegardent provisoirement ces informations dans des dispositifs personnels et les excluent après leur retour à l'entreprise, les backups de ces informations pourront rester indéfiniment dans des archives de données personnelles ou des unités de backup externes comme iCloud, Time Machine et autres systèmes de backup locaux basés automatiquement sur des nuages.

3. Maintenir des lieux de travail sécurisés

Recommander que les employés maintiennent isolés leur lieu de travail. Quand ce n'est pas possible, implanter ou rappeler aux employés les politiques existantes pour garder leur bureau propre. Par ailleurs, demander au secteur de TI de l'entreprise d'habiliter le blocage automatique d'écran sur tous les dispositifs de l'entreprise ou les fonctions de logout pour les serveurs personnels après de courtes périodes d'inactivité, exigeant un nom d'utilisateur et un mot de passe (et, si possible, authentification multi factorielle) pour récupérer l'accès. Enfin, dire aux employés de retirer ou déconnecter des appels confidentiels les haut-parleurs intelligents localisés près des mains; et de répondre aux appels dans un espace séparé des lieux communs de leur maison, y compris des membres de leur famille.

4. Restreindre le transport et l'impression de documents en dehors de l'entreprise

Restreindre la possibilité pour les employés d'imprimer des documents ou désactiver complètement la possibilité d'impression, particulièrement pour des documents qui contiennent ou décrivent des secrets professionnels. Dire aux employés de ranger les copies imprimées de documents confidentiels dans un lieu sûr jusqu'à ce qu'elle puissent etre rendues à l'entreprise. De la même façon, exiger que les copies des documents destinées à être jetées soient rangées dans une armoire ou un tiroir fermé à clé jusqu'à ce qu'elles soient détruites au moment de la réouverture de l'entreprise.

Pour les documents retirés de l'entreprise, instaurer un registre d'entrées et sorties pour les documents à rendre, et s'assurer qu'ils soient réellement rendus au moment de la réouverture de l'entreprise. De la même façon, instaurer un système de notification pour alerter le secteur de TI ou le contact désigné de l'entreprise à chaque fois que quelqu'un télécharge, copie, imprime, transfère ou exclut des données confidentielles ou des documents importants liés à un secret professionnel. Surveiller et enquêter sur toutes ces actions, même lorsqu'elles paraissent accidentelles ou innocentes.

5. Réseaux et dispositifs sécurisés

Dire aux employés d'ajouter une protection par mot de passe à leurs réseaux Wi-Fi personnels. Pour une protection supplémentaire, exiger que les dispositifs de l'entreprise soient toujours connectés au Réseau Virtuel Privé (VPN) de l'entreprise et instaurer l'authentification de deux facteurs pour accéder au VPN ou aux réseaux de l'entreprise. Par ailleurs, demander au TI d'envoyer un logiciel antivirus et malware pour ordinateurs portables et d'autres appareils de l'entreprise et désactiver USB et autres entrées externes sur les ordinateurs portables de l'entreprise pour empêcher l'envoi non autorisé de secrets professionnels et autres informations confidentielles, vers des clés USB ou des disques durs externes.

6. Limiter la transmission de documents et inclure des protections secondaires qui empêchent l'accès de destinataires non autorisés

Idéalement, les entreprises interdiraient la transmission de secrets professionnels ou autres informations ou documents confidentiels par e-mail ou autres moyens de transfert d'archives en dehors de leurs locaux. Toutefois, cette interdiction n'est sans doute pas réaliste dans les circonstances actuelles. Cependant, implanter des protections supplémentaires, exigeant qu'un destinataire d'email ait une adresse IP spécifique ou une signature numérique exclusive pour réviser des messages et des pièces jointes ouverts, empêchera qu'emails et pièces jointes ne soient envoyés, intentionnellement ou non, au mauvais destinataire et que les secrets professionnels qu'ils contiennent soient compromis.

D'autre part, les entreprises doivent limiter l'accès aux informations confidentielles selon les besoins. Par exemple, ne concéder l'accès qu'aux secrets professionnels importants et nécessaires à la réalisation d'un projet particulier et aux personnes y travaillant. Si possible, ne permettre l'accès au secret commercial ou à d'autres informations confidentielles qu'à travers des documents de collaboration archivés dans des unités de réseau interne sécurisées, ce qui réduira le risque de transmission indésirable à des tiers, de secrets professionnels ou autres informations confidentielles

7. Restreindre l'installation de logiciels non essentiels et de tiers

Comme les employés et leurs equipes utilisent différents moyens de communication et de connexion pendant le télétravail, les individus peuvent installer un logiciel apparemment sécurisé qui peut ouvrir des secrets professionnels et autres informations confidentielles. Considérant l'augmentation des activités criminelles dûe à la crise actuelle et le fait que les employés sont probablement plus distraits qu'en temps normal à cause de l'éducation à la maison, l'attention donnée aux enfants et le travail à temps complet, il est crucial que les entreprises surveillent constamment d'éventuelles nouvelles menaces et diffusent les menaces déjà connues. Pour éviter de nouvelles menaces, faire circuler celles déjà connues.

Pour obtenir une protection supplémentaire, prévoir l'adoption de procédures telles que le blocage à distance d'individus compromettant des secrets professionnels ou autres informations confidentielles, la destruction à distance de dispositifs installés dans des ordinateurs ou des téléphones égarés, ou dans le cas où un employé, un contractuel ou un fournisseur est incapable de le faire à cause de la maladie pendant qu'il travaille de chez lui.

8. Évaluer et adapter les protocoles de séparation des employés

Même si plusieurs entreprises ont déjà des procédures externes, ces procédures peuvent être difficiles à conclure à distance, particulièrement pour des entreprises qui font face à l'exclusion de plusieurs employés sur une courte période. Ainsi, les entreprises doivent être le plus prêtes possible à

conduire leurs procédures à distance, y compris: (i) en désactivant l'accès aux dispositifs et aux comptes de l'entreprise; (ii) en permettant le retour sécurisé de dispositifs, documents et autres biens de l'entreprise; (iii) en réalisant les entretiens de sortie par téléphone ou téléconférence; et (iv) en créant des versions numériques de contrats détaillant les obligations de confidentialité en vigueur signables électroniquement par les employés.

Retourner au texte principal

Photo: helloquence/Unsplash

› PROFESSIONNELS

Des professionnels qui allient vision juridique et compréhension du marché

Antonella Carminatti