Northbridge Assurance | CYBERSCOUT A TransUnion® Brand

PARLONS PRÉVENTION

INTERVENTIONS CRUCIALES EN CAS DE VIOLATION DES DONNÉES DE VOTRE ENTREPRISE

Aucune entreprise n'est à l'abri d'une atteinte à la protection de ses données, peu importe l'étendue de ses connaissances en cybersécurité. C'est pourquoi il est crucial de mettre en place un plan d'intervention en cas d'incident et de créer une documentation connexe. Dans votre plan d'intervention, vous devez inclure les mesures à prendre par votre entreprise si vous soupçonnez la violation de vos données. Plus vite votre entreprise suivra son plan en cas d'incident, mieux vous vous porterez et en meilleure posture vous serez pour atténuer l'incidence de la perte de données sur votre entreprise.

UNE ÉTUDE DE 2021 RÉALISÉE PAR IBM SUR LA CYBERRÉSILIENCE DES ENTREPRISES A RÉVÉLÉ QUE 54 % DES SOCIÉTÉS N'ONT PAS DE PLAN D'INTERVENTION APPLICABLE À L'ÉCHELLE DE LEUR ENTREPRISE EN CAS D'INCIDENT.

Pourtant, si on examine des cas récents de violation des données, on se rend compte qu'un large éventail d'entreprises sont ciblées par les cybercriminels : des PME aux multinationales, en passant par les organismes gouvernementaux. En outre, comme les incidents se multiplient de plus en plus rapidement de nos jours, de nombreux observateurs prévoient que la plupart des entreprises finiront tôt ou tard par être victimes d'un incident. C'est donc *maintenant* qu'il faut songer à préparer votre entreprise.

Formez votre équipe d'intervention en cas de violation des données

Votre personnel d'intervention clé doit être formé et bien comprendre ses responsabilités pour intervenir efficacement en cas de brèche de sécurité informatique. En détectant et en contenant une brèche informatique, une entreprise peut économiser beaucoup d'argent et éviter des conséquences négatives.

Au moment d'établir votre plan d'intervention en cas d'atteinte à la protection des données, vous devez penser à coordonner les activités de toutes vos équipes afin de réduire les risques d'erreurs.

Votre personnel de la sécurité et des technologies de l'information (TI) devrait constamment réévaluer les lacunes de l'entreprise concernant la sécurité des données, s'exercer à détecter les vulnérabilités et mettre en œuvre les mesures de sécurité, car il sera le premier à intervenir en cas de brèche informatique pour contenir l'incident et appliquer les correctifs. Selon l'étude *Cost of Data Breach* réalisée en 2021 par le Ponemon Institute d'IBM, le temps moyen pour repérer une brèche de sécurité informatique et la contenir est de 287 jours. Pour la période couverte par l'étude, les entreprises qui ont détecté la brèche de sécurité à l'intérieur de 200 jours, par opposition à celles qui ont mis plus de temps, ont économisé en moyenne plus d'un million de dollars.

L'équipe des services juridiques peut être amenée à travailler avec les TI, selon la gravité des incidents, pour déterminer les obligations légales de l'entreprise et fournir des conseils.

Les ressources humaines agiront en première ligne en cas d'incident pour communiquer avec les employés, surtout ceux dont les données personnelles auront été touchées. Elles peuvent aussi fournir des ressources aux employés et leur indiquer des façons de mieux se protéger, leur famille et eux (à la fois avant et après un incident de sécurité).

L'équipe des communications sera chargée d'informer les personnes touchées ainsi que la presse en cas d'incident. Elle collaborera avec l'équipe des services juridiques pour s'assurer que les communications sont exactes et produites en temps opportun. Le travail conjoint des deux équipes contribuera à réduire le risque que des amendes vous soient imposées par des gouvernements provinciaux ou fédéral, conformément à la réglementation en vigueur, par exemple la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* du Canada, et par des gouvernements étrangers, si vous avez des clients à l'extérieur du Canada.

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) fournit le cadre légal pour les avis que doit fournir votre entreprise. Toutes les organisations sont tenues de déclarer au commissaire à la protection de la vie privée du Canada (CPVP) les atteintes aux mesures de sécurité présentant un risque réel de préjudice grave (RRPG). En vous familiarisant avec les exigences légales, vous réduirez possiblement vos risques de litiges et d'amendes. De même, en respectant les délais pour l'envoi des avis, vous ferez preuve d'honnêteté, ce qui pourra vous aider à protéger la réputation de votre entreprise et à réduire la perte éventuelle de clients.

Établissez un plan de communication

En tant qu'entreprise de renom, vous avez la responsabilité d'informer les forces de l'ordre, les autres entreprises concernées, vos partenaires, vos employés et vos clients de toute divulgation potentielle de données après un incident. Les communications qui suivront peuvent viser à expliquer comment s'est produit l'incident, quelles données ont été compromises, quelles mesures ont été prises pour remédier à la situation et lesquelles seront prises pour protéger les personnes touchées.

Il est important de prendre note qu'il vous faudra désigner des porte-parole. Vous devrez les préparer à répondre aux questions, par exemple en leur fournissant une foire aux questions officielle, ainsi qu'aux demandes de renseignements transmises par téléphone, par courrier électronique, dans les médias sociaux ou dans la presse. Assurez-vous de faire preuve d'honnêteté dans vos communications et de répondre en temps opportun; cela pourrait vous aider à maintenir vos bonnes relations avec vos clients.

Renseignement et formation

Pour que votre stratégie d'intervention soit efficace, les membres de votre équipe d'intervention doivent faire des simulations pour s'exercer périodiquement à la mettre en œuvre. Ainsi, si un véritable incident survient, ils connaîtront les processus et les procédures à mettre en œuvre et seront prêts à passer à l'action. Lors de vos simulations, prêtez attention aux obstacles potentiels qui pourraient se dresser et apportez des améliorations d'une fois à l'autre.

En faisant des simulations régulièrement, votre entreprise sera mieux préparée à faire face à un incident réel.

Pour savoir comment mieux protéger votre entreprise, communiquez avec votre courtier d'assurance ou rendez-vous au **www.northbridgeassurance.ca**.

TROIS CONSEILS POUR SE PROTÉGER EN CAS DE BRÈCHE INFORMATIQUE

1. **Préparez-vous bien**
   N'attendez pas d'être victime d'une violation de données pour élaborer votre plan d'intervention.
2. **Protégez vos employés, vos clients et vos partenaires**
   Évaluez la possibilité d'inclure des outils de protection de l'identité dans l'arsenal de sécurité de votre entreprise et de ses parties prenantes.
3. **N'oubliez pas que c'est en forgeant qu'on devient forgeron**
   Vos employés doivent connaître votre plan d'intervention pour ne pas être pris au dépourvu si un véritable incident survient. Assurez-vous de leur faire faire des simulations pour bien les préparer.

[4051-001-ed03F | 05.2023]

Northbridge Assurance | CYBERSCOUT A TransUnion® Brand