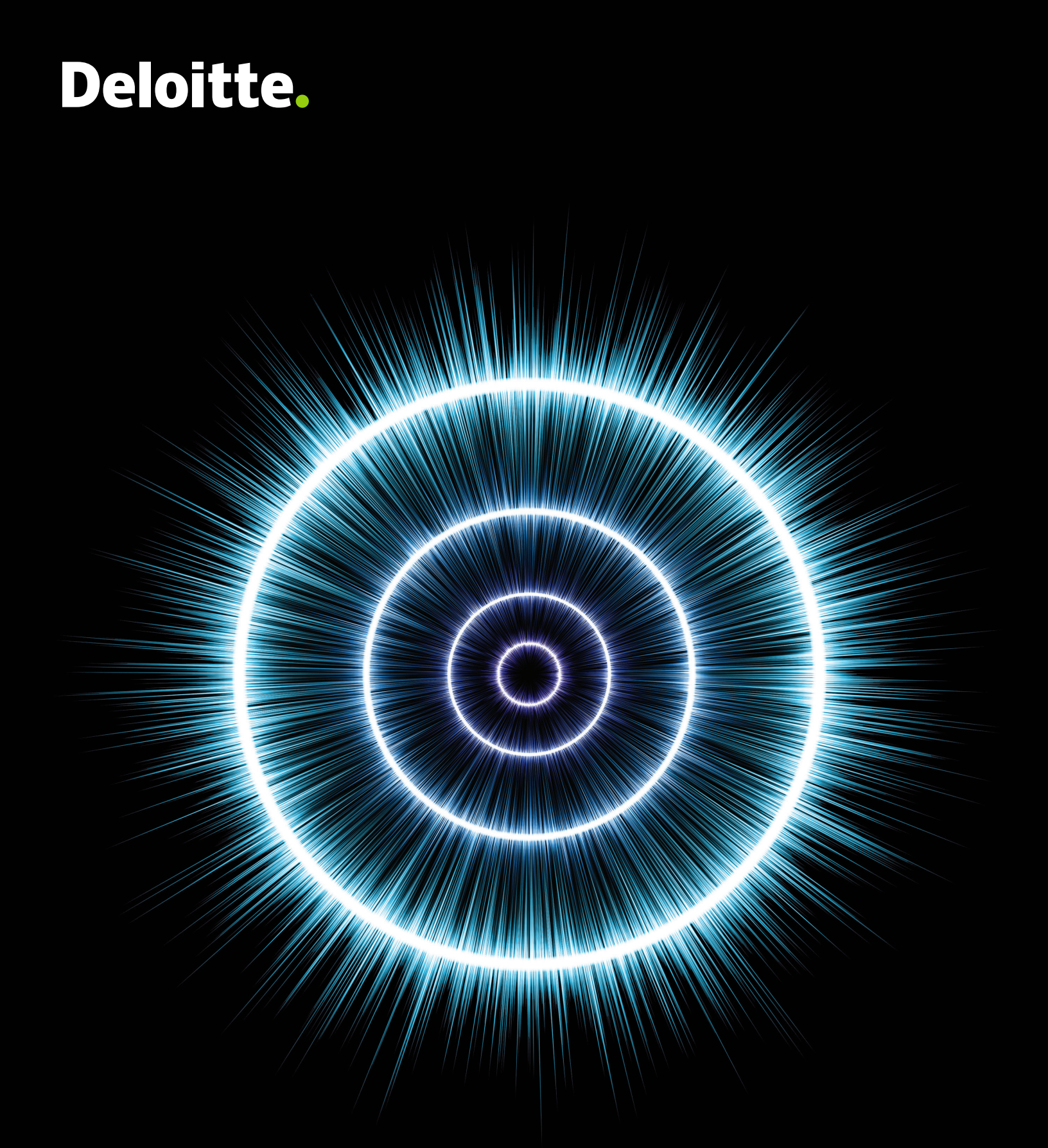
Deloitte.



Approche axée sur le client dans le cadre d'une violation des données

Aperçu des interventions

Résilience sous la pression

Demain, ce sera peut-être à votre tour d'être victime d'une violation de données et de faire les manchettes.

Nous savons pertinement qu'à peu près toutes les entreprises subiront tôt ou tard une violation de données. Ce qui veut dire que la plupart des clients le savent aussi, et qu'ils s'attendent à ce que les sociétés avec lesquelles ils font affaire soient minutieusement préparées à réagir rapidement et efficacement à la plus petite brèche qui soit dans leur forteresse de cybersécurité. De même, ils veulent être tenus au courant et savoir sur-le-champ si leurs données ont été touchées, pas dans un mois ou plus.

De nouvelles lois sévères liées au respect de la vie privée au Canada et dans l'Union européenne contraignent davantage les organisations à protéger suffisamment les données de leurs clients. En effet, vos clients comptent sur vous pour prévenir ce qui est évitable et vous préparer à l'inévitable. Et ce n'est pas une tâche impossible.

Lisez la suite pour savoir comment vous pouvez justifier la confiance que vos clients vous accordent en leur donnant la priorité si jamais un incident lié à la violation de données survient, notamment grâce à des notifications rapides et à une intervention de qualité, ce qui passe par une infrastructure solide, des processus et des systèmes efficaces et une exécution professionnelle.

Une fois les données perdues, c'est le client qui a besoin d'être protégé

Les cyberincidents étant de plus en plus médiatisés, les organisations prennent conscience qu'elles pourraient être la prochaine cible de violation des données à défrayer la chronique.

De lois et normes récentes sur la protection des données, telles que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) au Canada et le *Règlement général sur la protection des données* (RGPD) de l'Union européenne, qui s'étend aux pays hors de l'Europe, ont mis en lumière comment les entreprises se préparent et répondent à une violation de données. Mais lorsqu'elles subissent un tel incident, bon nombre d'entreprises consacreront instinctivement leurs ressources et leurs efforts à contenir la faille, plutôt qu'à leur plus important atout : leurs clients.

Lorsque l'ampleur de la violation est rendue publique, les organisations qui possèdent d'importantes bases de données de clients et qui n'accordent pas la priorité aux besoins des clients risquent d'amplifier la crise de manière exponentielle.

Si elles ne gèrent pas les répercussions sur les clients, elles sont susceptibles de subir des conséquences très médiatisées, comme des amendes réglementaires et la perte de clients, ce qui pourrait nuire à la valeur et à la réputation de la marque, augmenter le risque de démissions chez les dirigeants, et accélérer la dégringolade du cours de l'action.

Si le pire devait arriver, comment une entreprise peut-elle s'assurer qu'elle est prête à réagir et à protéger ses clients?

Ce document, qui fait partie d'une série de perspectives de Deloitte pour les interventions en cas de crise, se penche sur les défis liés aux clients que les organisations canadiennes doivent relever à la lumière de la LPRPDE et du RGPD, et dégage les facteurs qui contribuent à une intervention efficace, axée sur le client, en cas d'atteinte à la sécurité des données.

Approche axée sur le client dans le cadre d'une violation des données | Une fois les données perdues, c'est le client qui a besoin d'être protégé

Plus de **2,5 milliards** de dossiers ont été perdus par des entreprises mondiales en 2017, soit une hausse de

88 %

par rapport à 2016[1]

[1] Gemalto, indice des niveaux de violation

Avant la violation : se préparer à l'inévitable

Le RGPD et la LPRPDE prescrivent aux organisations de mettre en place des mesures appropriées dans le cadre de leurs activités de préparation aux violations et de tenir un dossier de toutes les violations.

Ces mesures nécessitent un plan d'intervention qui comprend, entre autres facteurs, la notification des clients dans les meilleurs délais en cas de violation susceptible d'entraîner des risques élevés liés à la protection de la vie privée ou de présenter un risque réel de préjudice grave.

Pour expliquer ce que cela pourrait signifier pour la plupart des organisations, le graphique figurant à la page suivante examine les répercussions d'une violation du point de vue des principaux **défis** qui sont susceptibles d'en découler.

Dès lors qu'une entreprise comprend qu'elle a été victime d'une violation de données, les minutes sont comptées.

Selon un rapport publié en 2018 par le Ponemon Institute sur le coût des violations de données, il a fallu **197 jours** en moyenne avant que les entreprises se rendent compte qu'elles avaient été victimes d'une violation[2].

Incidence sur les clients :
reconnaître les risques réels auxquels les clients sont exposés

Trop souvent, les entreprises ne comprennent pas vraiment que les risques réels auxquels les clients sont exposés se manifestent dans les jours et les semaines qui suivent la violation, au moment où des criminels pourraient utiliser les données volées pour accéder aux comptes compromis des clients, en plus de chercher à les frauder par des techniques d'hameçonnage et d'escroquerie par courriel ou par téléphone.

Aussi, aviser les clients de la violation n'est que la première étape d'une très longue démarche. Ce qui compte vraiment, c'est de les soutenir et de les protéger durant les jours et les semaines qui suivent l'incident.

Rapidité :
mobiliser des capacités d'intervention en cas de violation

Dès lors qu'une entreprise comprend[2] qu'elle a été victime d'une violation de données, les minutes sont comptées.

Inévitablement, les attentes découlant du délai de notification réglementaire de 72 heures en vertu du RGPD sont susceptibles de contraindre les entreprises à précipiter leur échéancier; aussi, la mobilisation des capacités ayant l'envergure nécessaire à une intervention adéquate auprès des clients devient une course contre la montre hautement visible et très risquée si l'entreprise n'est pas bien préparée.

[2] 2018, étude sur les coûts d'une violation de données, rapport de recherche du Ponemon Institute. Commandité par IBM Security.

Approche axée sur le client dans le cadre d'une violation des données | Avant la violation : se préparer à l'inévitable

Capacité :
assurer une intervention en cas de violation tout en poursuivant les activités

Une violation est susceptible de provoquer une augmentation considérable de la demande envers les opérations internes de l'organisation; aussi, l'un des premiers défis consistera à s'assurer d'avoir suffisamment de ressources pour poursuivre les activités normales, en plus de mettre sur pied une mission d'intervention efficace.

Un enjeu élevé lié à la capacité sera de gérer la forte hausse probable des communications provenant de clients inquiets. De longues attentes au téléphone se traduisent rapidement par des commentaires négatifs dans les médias sociaux et une couverture médiatique sur les clients frustrés.

Compétences :
spécialistes détenant l'expérience et les compétences en violation

Plus que toute autre crise, une violation de données nécessite un groupe important de spécialistes pour assurer une intervention fructueuse auprès des clients : experts en communication avec les clients, analystes des médias sociaux, spécialistes opérationnels, experts en cyberintervention et enquêteurs en juricomptabilité, entre autres.

Et bien entendu, ces nombreuses ressources de soutien doivent être coordonnées et gérées avec minutie, pour assurer que le bon soutien est offert au client, de la bonne manière et au bon moment.

Infrastructure :
soutien technique et logistique

La disponibilité d'une infrastructure clé pour permettre une intervention rapide en cas de violation est essentielle. Une capacité téléphonique suffisante, des technologies habilitantes et une structure opérationnelle claire sont déterminantes pour répondre à la hausse certaine de la demande des clients.

Une assistance logistique est également nécessaire dans des domaines de soutien clés. Les capacités d'impression et d'envoi à grande échelle ainsi que les services de surveillance du crédit, par exemple, doivent tous être prêts à fonctionner, et les contrats connexes doivent déjà être en place.

Après la violation : atténuer l'incidence sur le client

Facteurs d'intervention essentiels

En fin de compte, l'issue d'une réponse en cas de violation est déterminée par deux facteurs : les notifications rapides et la qualité de l'intervention.

Rapidité des notifications

Évaluée selon le nombre d'heures entre le moment où l'on prend connaissance de la violation et le moment où les organismes de réglementation et les clients sont avisés.

Qualité des interventions :

Évaluée selon la capacité de l'organisation à exécuter avec succès chaque volet du plan, à l'échelle nécessaire et en situation de crise.

L'essentiel, c'est de continuer d'accorder la priorité au client pendant et après la violation.

Rapidité des notifications

La vitesse à laquelle une entreprise peut aviser les clients en cas de violation et l'exactitude des renseignements reposent sur la disponibilité de ressources modulables, l'infrastructure en place pour répondre à la hausse d'activités qui s'ensuit et la qualité des interventions.

En pratique, cela signifie :

1. Une équipe de réserve modulable, dont la mobilisation immédiate est garantie lorsqu'une violation survient pour assurer un soutien efficace aux clients.

2. Les outils, processus et systèmes nécessaires pour gérer le processus d'engagement des clients dans les semaines qui suivent la violation.

Aussi efficaces soient-ils, les plans d'intervention ne gagneront pas la course aux notifications si des capacités et une infrastructure adéquates n'ont pas été mises en place pour assurer leur exécution.

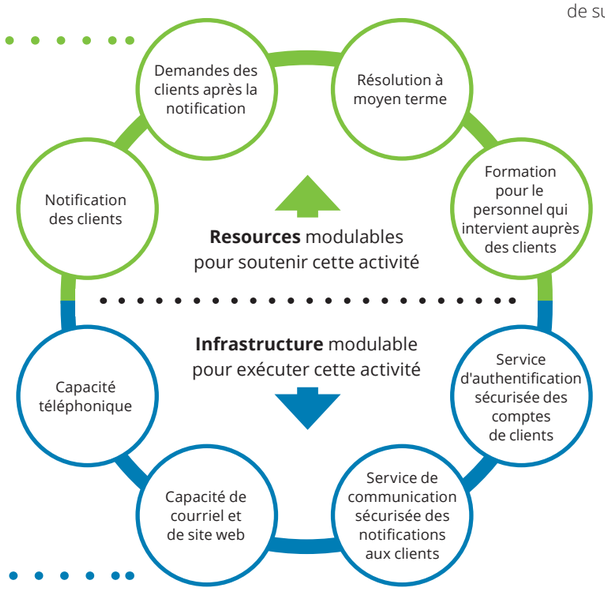
Les plans fructueux qui sont axés sur le client tiennent compte du nombre de **ressources chevronnées** nécessaires pour permettre à tous les clients à risque d'être avisés, répondre aux questions et gérer les préoccupations des clients, et remédier à toute activité frauduleuse suspectée.

Les plans efficaces tiennent aussi compte de **l'envergure de l'infrastructure** nécessaire pour assurer les notifications en cas de violation, notamment :

- **Des systèmes de notifications sortantes** dotés de capacités de courrier de première classe à grand volume et d'hébergement de site web à haute capacité aux fins d'intervention.

- **Des outils de communications entrantes** et un système téléphonique à haute capacité pour acheminer rapidement les appels et les courriels des clients en toute sécurité.

- **Une plate-forme de protection de l'identité** comportant la restauration de l'identité des clients, des systèmes de surveillance et une assurance.



Qualité des interventions

Le deuxième facteur de réussite est le niveau de **compétences spécialisées** et d'**expérience** de l'équipe d'intervention.

Les exigences de la LPRPDE et du RGPD ont principalement trait à la confidentialité des données et à la notification en temps voulu des violations. Cependant, une notification rapide dont le niveau de détail n'est pas approprié peut augmenter la frustration des clients et ainsi, alimenter les publications cinglantes dans les médias sociaux, la visibilité dans les médias, et les litiges. Par ailleurs, l'absence d'information forcera sans doute l'organisation à émettre d'autres notifications à mesure que les détails se font connaître, et elle continuera de susciter la frustration chez ses clients et de faire les manchettes pour les mauvaises raisons. La qualité des interventions est influencée par la capacité de l'organisation à enquêter sur de grands volumes de données de manière efficiente et efficace. La plupart des données atteintes se trouvent dans des bases de données, où elles côtoient des renseignements confidentiels permettant d'identifier des personnes, des renseignements en matière de soins de santé, des données financières, des comptes de médias sociaux, des noms d'utilisateur et des mots de passe.

De plus en plus de reportages dans les médias font état de violations dont le nombre de dossiers touchés est « inconnu » et de renseignements qui ont « peut-être » été compromis. Ces énoncés sont des exemples d'atteintes à la sécurité des données où il était impossible de déterminer le nombre de dossiers touchés. Lorsqu'elle ne peut pas démontrer le contraire, une organisation est souvent contrainte de présumer que tous les renseignements ont pu être compromis durant la violation. Cela vient compliquer la clarté des messages aux clients et accroître les répercussions associées à la violation.

Heureusement, il existe une méthode d'enquête approfondie qui peut aider les organisations à cerner les dossiers précis des clients qui sont touchés par une violation, leur permettant de limiter l'incidence de la violation et de transmettre des messages clairs aux clients. Cette méthode, appelée investigation numérique de bases de données, consiste en une enquête approfondie des technologies de base de données. Elle détermine avec précision les dossiers touchés par une violation, permettant aux entreprises de prendre des mesures pour réduire l'ampleur et les conséquences de la violation. Dans certains cas, elle peut démontrer que les renseignements visés par l'exigence de notification n'ont pas été compromis; le cas échéant, les organisations ne sont pas tenues de rendre l'incident public.

Approche axée sur le client dans le cadre d'une violation des données | Qualité des interventions

L'enquête approfondie peut contribuer à réduire l'ampleur et les conséquences d'une violation. Dans certains cas, les organisations ne seront pas tenues de rendre l'incident public.

Le graphique à la page 14 met en lumière les facteurs d'incidence les plus évidents qui sont associés à une violation de données, tels que les enquêtes techniques et les notifications aux clients, et ceux qui sont couramment ignorés et qui entraînent des coûts cachés.

Les organisations qui souhaitent obtenir une expertise en investigation numérique de bases de données devraient s'assurer que leurs fournisseurs potentiels possèdent des outils évolués, des compétences et des experts crédibles qui peuvent défendre leurs conclusions dans le cadre d'actions en justice. Les fournisseurs et les experts ne sont pas tous aussi expérimentés dans ce domaine; aussi, les organisations doivent faire leurs devoirs avant de retenir les services d'un fournisseur.

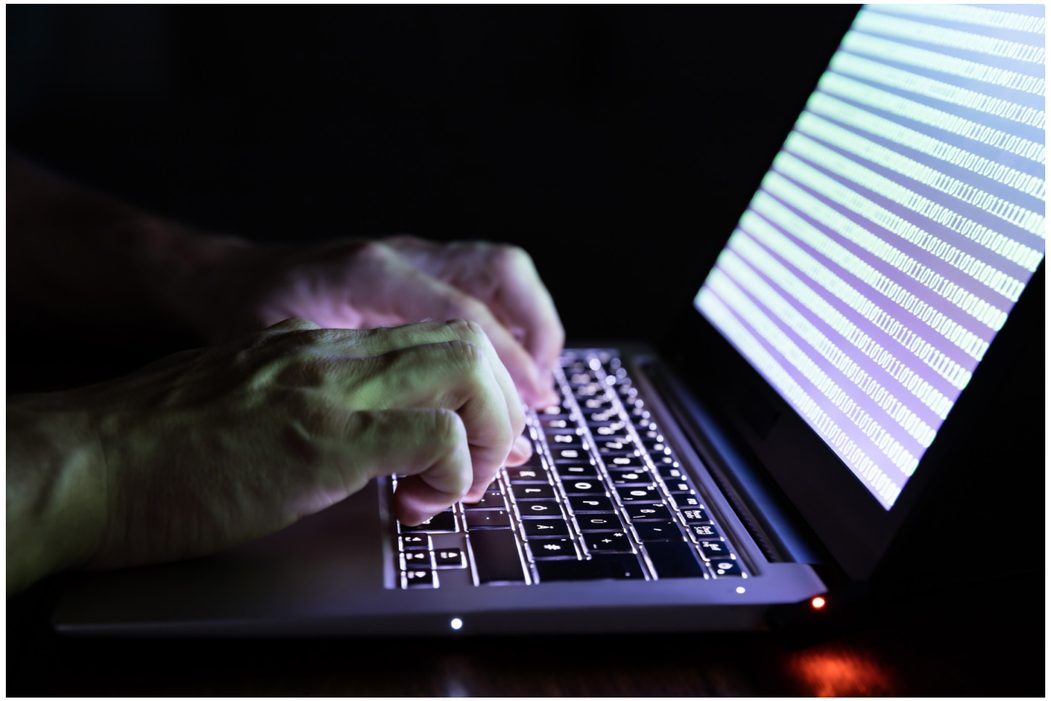
En plus de recueillir l'information appropriée pour rédiger les messages de notification d'une violation, les organisations doivent se doter d'une stratégie complète de protection de l'identité, allant de l'accès au suivi du crédit et des alertes de fraude aux services de soutien à la restauration de l'identité. Ce genre de soutien peut grandement contribuer à atténuer les préoccupations des clients, et à les rassurer que tout a été mis en œuvre pour les protéger en cette période de vulnérabilité.

En résumé, une stratégie d'engagement des clients gérée minutieusement est essentielle pour assurer une intervention efficace en cas de violation de données. Aussi, la qualité et la sensibilisation du personnel qui interagit avec les clients dans les centres de contact sont primordiales; leur capacité de trier les besoins des différents clients, de fournir des conseils et du soutien en matière de protection de l'identité et de contribuer à la restauration de l'identité est essentielle à la mise en œuvre fructueuse de la stratégie d'engagement des clients. Souvent, cette responsabilité est confiée à des professionnels pour accélérer la prise de mesures et améliorer le service à la clientèle offert par les personnes qui s'acquittent régulièrement de cette tâche. L'incapacité de gérer et de prendre soin du client signifie l'incapacité de gérer la réputation de l'organisation.

Réduire l'incidence des violations de données

Les bases de données spécialisées et l'investigation numérique des données massives peuvent aider les organisations à mieux atténuer ou cerner les violations de données précises des clients. Cela peut limiter l'incidence de la violation au seul coût de l'enquête technique ou la diminuer pour l'ensemble des éléments présentés dans l'infographique.

Approche axée sur le client dans le cadre d'une violation des données | Réduire l'incidence des violations de données



Il est presque inévitable que les organisations composent tôt ou tard avec une violation de données, mais ce n'est pas impossible d'éviter des conséquences telles que la perte de clients et des manchettes portant atteinte à leur réputation.

Stratégie axée sur le client : planification réfléchie

Les interventions à la suite d'une violation importante des données des clients sont plus complexes que la plupart des entreprises ne le croient. Aussi, peu d'organisations possèdent l'infrastructure, les ressources et les connaissances spécialisées voulues pour gérer les retombées par elles-mêmes.

Une intervention axée sur le client et fondée sur les meilleures pratiques permet de protéger les clients, de réduire au minimum les risques réglementaires et liés à la réputation, et de diminuer l'incidence financière globale d'une atteinte à la sécurité des données. Mais un déploiement au rythme dicté par les lois canadienne et européenne n'est possible qu'en élaborant une planification efficace avant qu'une violation se produise. Les organisations doivent s'assurer d'avoir à leur disposition les ressources appropriées pour traiter le volume de demande des clients, et se doter d'une infrastructure sécurisée et modulable offrant le meilleur service qui soit à ceux auxquels appartient l'avenir de l'entreprise : les clients.

À la suite d'une violation de données, le soutien aux clients est crucial, complexe et grandement sous-évalué. Un service à la clientèle très performant réduit au minimum les éventuels dommages aux clients découlant de toute activité criminelle et contribue à atténuer les amendes en vertu de la LPRPDE et du RGPD.

Ces services de soutien réduisent également la possibilité d'atteinte à la réputation et améliorent la fidélisation des clients. Parce que des clients qui bénéficient d'un excellent soutien sont moins susceptibles de passer à d'autres organisations.

Il est presque inévitable que les organisations composent tôt ou tard avec une violation de données, mais il n'est pas impossible d'éviter des conséquences telles que la perte de clients et des manchettes portant atteinte à leur réputation.

Il est essentiel d'adopter une approche axée sur le client pour la planification et l'intervention en cas de violation de données afin de parvenir à une issue positive à une situation potentiellement désastreuse.

Personnes-ressources

Pour en savoir davantage, communiquez avec :

Kevvie Fowler
Associé, leader mondial, Intervention en cas de cyberincident et leader canadien, Résilience
905-767-8067
kfowler@deloitte.ca

Robert Masse
Associé
514-393-7003
rmasse@deloitte.ca

Vous êtes victime d'un cyberincident?
Appelez notre ligne d'assistance en cas d'incident :
1-833-DELOITTE (335-6488)

Notes

Deloitte.

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans de nombreux secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500[MD] par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte ont une influence marquante — y compris les 9 400 professionnels au Canada — veuillez nous suivre sur LinkedIn, Twitter ou Facebook.

Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

 18-6089T