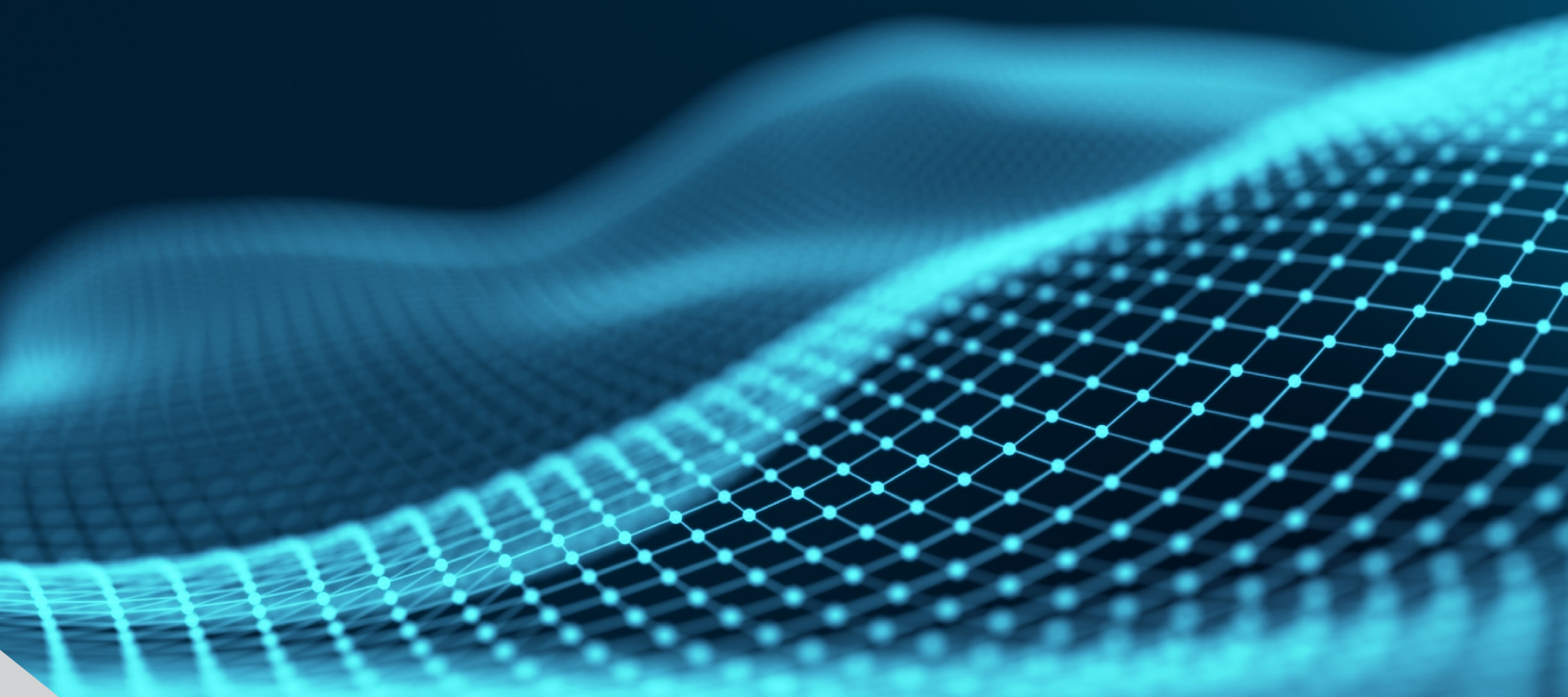
CYBERSÉCURITÉ ET
COMMUNICATIONS DE CRISE

Comment naviguer efficacement et se préparer à une cyberattaque

Mars 2021



N|A|T|I|O|N|A|L

RÉDIGÉ PAR :
Karen White, vice-présidente, Gestion de crises et d'enjeux
Larry Markowitz, conseiller spécial, Communication financière et relations investisseurs
Odane Finnegan, chargé de projets, Affaires publiques

Aperçu

Chez NATIONAL, nous savons qu'une bonne exécution repose sur une bonne planification, et que cette règle est amplifiée en fonction de l'intensité d'une crise.

Il n'y a sans doute pas de crise plus grave pour une organisation qu'une atteinte à sa cybersécurité. Quel que soit le secteur d'activité, la sécurité des données de vos clients est essentielle à la santé de votre relation avec ceux-ci. Alors que l'environnement de travail devient de plus en plus numérique, de nouvelles voies d'attaques perpétrées par des cyberacteurs malveillants se sont ouvertes. **À la lumière de cette nouvelle réalité, nous avons décidé de partager certaines pratiques exemplaires à appliquer lorsque (et non pas au cas où) votre organisation sera confrontée à une crise de cybersécurité.**

Le nouvel environnement

Les données voyagent rapidement. Alors que s'effectue la transition vers une culture du travail à domicile privilégiant le numérique, votre environnement numérique doit devenir une priorité pour les décideurs de votre organisation. Dans cette section, nous mettrons en évidence les risques accrus que présente l'infrastructure standard actuelle. Nous décrirons les récentes transitions dans l'environnement réglementaire ainsi que les changements dans les perceptions des consommateurs.

Nouveaux vecteurs d'attaque

Commençons par une évidence : l'année dernière a changé le monde. Dans tous les aspects de la vie, les événements des douze derniers mois ont modifié les procédures opérationnelles habituelles pour tous. L'un de ces changements fut l'adoption à grande échelle de protocoles de travail à domicile pour les entreprises de toutes tailles. Alors que les employés se branchaient depuis leur domicile, le nombre de points d'entrée pouvant permettre l'infiltration d'acteurs indésirables a augmenté drastiquement. Les réseaux domestiques individuels sont plus susceptibles d'être attaqués pour de nombreuses raisons (que nous n'examinerons pas dans cet article). Cela s'est traduit par une augmentation significative des tentatives d'attaques des réseaux d'entreprise.

Selon le rapport de l'ACEI sur la cybersécurité, trois organisations sur dix ont constaté une hausse du volume d'attaques pendant la pandémie. Ce chiffre représente probablement une estimation prudente, car cette même enquête révèle que 38 % des répondants ne savaient même pas si les données de leurs clients et/ou employés avaient été affectées par une intrusion au cours de l'année écoulée. En effet, nous avons vu de nombreuses intrusions n'être révélées qu'après la découverte d'une liste de données confidentielles de clients sur le « Web clandestin » (*dark Web*).

Face à une telle incertitude, comment sauriez-vous si vos données ont été exfiltrées? Cela nécessite un examen approfondi des pratiques actuelles de stockage et de partage des données, ainsi qu'un processus permettant d'identifier les cas où quelque chose est survenu en dehors des pratiques standards. Notre travail devenant de plus en plus virtuel, l'importance de protéger l'information vulnérable n'a jamais été aussi grande, que vous soyez dans le secteur privé ou dans le secteur public.

Les organisations qui stockent des informations sur leurs clients ou leurs employés (en d'autres termes, toutes les organisations) doivent être parfaitement conscientes des répercussions qu'une fuite de données ou un autre incident de cybersécurité aurait sur leurs activités et leur réputation. Elles doivent planifier en conséquence et comprendre les mesures à prendre (a) avant qu'un incident ne se produise, (b) pendant qu'il se produit, et (c) après qu'il ait pris fin.

Changements réglementaires

Une fois un enjeu identifié, une litanie de questions s'ensuit. Il existe cependant une série de questions pour lesquelles les réponses ont considérablement changé ces derniers temps : que suis-je légalement tenu de faire? Qui dois-je informer? Dans quel délai?

Les législateurs fédéraux et provinciaux ont instauré des attentes claires pour les organisations victimes d'une intrusion : communiquer clairement, honnêtement et souvent. Les cyberattaques qui portent atteinte aux renseignements personnels identifiables (RPI) étant de plus en plus fréquentes, les gouvernements ont reconnu la nécessité de mettre à jour la législation afin de protéger leurs citoyens.

Le 17 novembre 2020, le gouvernement fédéral a déposé le projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte numérique, qui vise à remanier considérablement les lois fédérales canadiennes sur la protection de la vie privée, en offrant aux individus un plus grand contrôle sur leurs données et en tenant les entreprises qui traitent des données personnelles responsables de la protection de ces données. Le projet de loi crée un nouveau cadre de gestion des données en vertu duquel les consommateurs se voient accorder un contrôle accru sur la façon dont leurs données sont utilisées et doivent consentir à toute diminution de ce contrôle. Le nouveau régime d'application représente un changement important par rapport au système précédent. Il prévoit des amendes importantes pouvant atteindre 10 millions de dollars ou 3 % du chiffre d'affaires mondial pour les entreprises qui ne protègent pas les données de leurs utilisateurs, ce qui signifie que la protection des données et de la vie privée des Canadiens deviendra une priorité plus importante pour les organisations.

L'évolution des attentes des consommateurs

Il existe un adage dans la Silicon Valley qui va comme suit : « Si l'application est gratuite, vous êtes le produit ». Tirer profit du temps d'utilisation d'une application ou d'une plateforme est devenu la caractéristique dominante de notre économie numérique. Cependant, les utilisateurs ont souvent le sentiment de n'avoir aucun contrôle sur leur empreinte numérique. Par conséquent, lorsque des violations de données ont commencé à être mises au jour, les consommateurs ont réagi de manière impitoyable.

Une enquête commanditée par le Commissaire à la protection de la vie privée du Canada a révélé que la proportion de Canadiens qui ont ajusté les paramètres de leur appareil pour limiter la quantité d'informations personnelles partagées avait augmenté de façon constante, passant de 40 % en 2011 à un sommet de 76 % en 2016. De plus, 82 % des répondants ont indiqué qu'ils désinstalleraient une application en fonction des renseignements qu'elle demande; 92 % ont exprimé un certain niveau d'inquiétude quant à la protection de leur vie privée; et près de 60 % sont préoccupés par la possibilité que leurs publications sur les médias sociaux nuisent à leur réputation. Ces chiffres sont révélateurs de l'importance du contrôle de l'utilisation et de la confidentialité des données personnelles.

Ce désir de contrôle ne concerne pas seulement les questions de sécurité. Un autre ajout notable à cette enquête menée par le Commissaire à la protection de la vie privée du Canada fut l'opinion du public à propos de l'économie des données telle qu'elle existe en ce moment. Les trois principales préoccupations énumérées étaient : les entreprises comme les fournisseurs d'assurance qui utilisent les données les concernant pour prendre des décisions; les agences de marketing qui analysent les goûts et les préférences pour cibler la publicité; et les renseignements personnels utilisés dans le cadre d'un processus d'embauche. Le niveau de connaissance et de sensibilisation des consommateurs augmente et, à mesure que cela se produit, ils s'attendent à un niveau de clarté de la part des entreprises et des organisations avec lesquelles ils interagissent.

Malgré tout ce qui précède, ce rapport contient quelques bonnes nouvelles pour les entreprises. L'enquête souligne quelques domaines clés sur lesquels les chefs d'entreprise peuvent se concentrer pour améliorer la confiance et l'engagement envers leurs plateformes, produits et services. À une question au sujet des pratiques ou lois qui devraient être prioritaires, deux réponses ont récolté un appui de plus de 70 %. La première était de s'assurer que les entreprises se verraient infliger une pénalité financière « importante » en vertu de la loi canadienne, avec la possibilité d'imposer des amendes allant jusqu'à 5 % des revenus mondiaux. La seconde était que les Canadiens étaient « certainement » ou « probablement » plus disposés à transiger avec une entreprise si celle-ci « fournit des informations claires et faciles à comprendre sur ses pratiques en matière de confidentialité ».

Élaborer votre plan de contingence en cybersécurité

Forts d'une meilleure compréhension du paysage réglementaire et des attentes des consommateurs, il appartient aux dirigeants d'entreprise de mettre en œuvre les meilleures pratiques éprouvées.

Une atteinte à la protection des données est un moment critique pour toute organisation. Votre réaction et la façon dont vous la communiquez auront un impact sur l'identité de votre marque, en bien ou en mal.

Chez NATIONAL, nous avons identifié plusieurs pratiques exemplaires que vous pouvez mettre en œuvre en cas d'atteinte aux données. Nous avons divisé ces recommandations en trois catégories : (a) ce que vous pouvez faire immédiatement, (b) ce que vous pouvez faire pendant une attaque, et (c) ce que vous devez faire après avoir identifié les problèmes et contenu l'atteinte.

Avant la cyberattaque

Puisque vous ne souhaitiez sûrement pas « construire votre avion en vol », il est préférable de faire un peu de planification avant d'être victime d'une cyberattaque ou d'une autre forme d'atteinte aux données.

Prendre le temps de vérifier et de réfléchir aux vulnérabilités, à l'état de préparation, aux procédures et aux ressources de votre organisation en matière de communication de crise constitue une étape essentielle de la planification avant l'événement. Cela vous permettra de découvrir des lacunes relatives à l'état actuel de préparation et de formuler des recommandations et des actions. Les conclusions de la phase d'audit préattaque, qui comprend généralement la consultation d'experts en droit, en sécurité et en technologies de l'information afin d'examiner et de renforcer le manuel de cyberintervention de votre organisation, vous aideront à anticiper et à gérer les problèmes susceptibles de prêter flanc à une atteinte aux données.

Maintenant, que devrait comprendre votre document en cas de cyberattaque? Commencez par une liste de questions. Cela vous permettra de chercher au sein de votre organisation – et à l'extérieur de celle-ci – les personnes qui pourront vous aider à y répondre. En suivant ce processus et en répondant à ces questions, vous pourrez élaborer votre réponse future à tout problème de sécurité ou d'atteinte aux données. Vous aurez commencé à construire votre avion avant qu'il ne doive « prendre son envol ». À cette fin, nous avons cru bon vous aider à développer certaines des questions que vous devriez poser.

La première question est : quelles sont les données en notre possession? Cela peut sembler simple, mais il peut y avoir plusieurs réponses à cette question en fonction de la taille de votre organisation. Si c'est le cas, votre premier objectif devrait consister à formuler une réponse applicable à l'échelle de toute l'organisation. Même si tout le monde n'a pas accès à l'ensemble des données, il est important de savoir quelles informations sur les clients sont conservées et où elles le sont. La nature des données que vous conservez influencera le reste du processus, car différents types de données nécessitent différents niveaux de protocoles de sécurité. Conservez-vous simplement un carnet de commandes? Ces données sont-elles associées à une carte de crédit ou à d'autres informations de paiement?

Ensuite, vous devez évaluer où ces données sont conservées et la nature des protocoles en place pour déterminer quand et où une atteinte aux données s'est produite. Il y a d'autres questions techniques à poser et auxquelles il faut répondre, concernant les mots de passe, les intégrations de tiers, et toute une liste à travers laquelle les experts en données et en confidentialité pourraient vous aider à naviguer. En ce qui nous concerne, puisque nous examinons la façon de communiquer pendant cette période et de s'y préparer au mieux, nous devons aborder ces questions afin d'avoir une meilleure compréhension du niveau de risque auquel vous êtes confronté et des enjeux potentiels qui peuvent en découler.

L'objectif final lors de la création d'un programme de conformité est d'avoir une compréhension fondamentale des risques auxquels vous êtes exposés et des mesures concrètes mises en place pour atténuer les risques potentiels. En répondant à ces questions, vous aurez établi le cadre permettant de rédiger vos communications et de déterminer les scénarios de risque. Une fois cette planification complétée, vous devriez disposer d'un dossier à la fois sécurisé et accessible en tout temps (la dernière chose que vous souhaitez est de créer un plan, puis de le voir verrouillé par un pirate). Ce dossier traitera de vos préoccupations en matière de données, de la nature des données en votre possession, de l'endroit où vous les conservez et de la façon elles sont conservées en toute sécurité. Votre dossier contiendra votre liste de contacts immédiats et une liste de vérification comportant des questions, telles que :

» Quels sont les publics touchés par cet incident?

» Avons-nous prévenu les employés? Les clients?

» Avons-nous informé les autorités réglementaires? Quelles sont les notifications requises?

» Que disons-nous à chaque groupe de parties prenantes?

» Quand devons-nous communiquer? Et à quelle fréquence?

» Comment saurons-nous si nous avons réussi?

Toutes ces questions contribueront à alimenter vos listes de vérification et votre plan de préparation en cas de crise. Elles constitueront également la base servant à tester votre plan de crise afin que vous soyez prêt à réagir en cas de cyberattaque.

LA PLANIFICATION PRÉALABLE À LA CYBERATTAQUE COMPREND :

- ✓ Une vérification globale de la préparation aux crises
- ✓ Une vérification de la planification et du matériel de communication
- ✓ Une analyse et une recherche sur les médias sociaux et traditionnels
- ✓ Une formation des cadres et une formation média
- ✓ L'élaboration d'un guide pour les cybercrises comprenant :
  - » L'élaboration de scénarios
  - » Une équipe de crise et des protocoles d'approbation établis
  - » Des porte-parole identifiés
  - » L'identification et la priorisation des publics et des canaux de communication
  - » L'élaboration de messages clés
  - » Les paramètres de mesure et d'évaluation
- ✓ Les exercices de simulations de crise

Pendant la brèche de sécurité

Armées d'un guide de gestion des crises, les organisations peuvent immédiatement faire appel à leur équipe d'experts en communication de crise, en affaires juridiques, en assurance et en cybersécurité pour faire face aux cyberincidents.

Les cyberincidents peuvent être perturbateurs et avoir un impact sur les affaires de l'entreprise et la poursuite de ses activités. De nombreuses organisations sont en mesure de créer efficacement une cellule de crise virtuelle ou présentielle, ou un centre de mesures d'urgence, et de mobiliser du personnel expérimenté pour gérer efficacement toutes les composantes de la crise, notamment les technologies de l'information, les opérations, les ressources humaines, les services juridiques, les assurances et les communications. Lorsqu'une brèche survient, trois grandes préoccupations se présentent aussitôt :

» Comment pouvons-nous sécuriser nos données et les protéger contre cette attaque?
» Quelle est la nature des données qui ont été compromises?
» Quelles sont les personnes ou les parties prenantes touchées par cet incident, et comment allons-nous communiquer avec elles?

Quelles que soient les circonstances de l'incident, le premier principe de base est le suivant : les **communications doivent être précises et opportunes**. Par opportunes, nous voulons dire qu'il est important de comprendre, à partir de votre enquête, quels sont les publics touchés et quelle est la nature des données qui ont été compromises. Si des renseignements personnels ont été compromis, cela entraînera des exigences réglementaires plus formelles en matière de notification. En gardant le silence, on risque de créer un vide qui sera comblé par des rumeurs et des spéculations. Au fil de votre enquête et de votre compréhension de ce qui s'est passé, vous pouvez mettre à jour votre communication initiale en y ajoutant des détails pertinents. Tout ce que vous dites doit être exact et concis; de plus, les renseignements que vous communiquez doivent être cohérents et transmis à des fins précises.

Le deuxième principe consiste à **communiquer directement avec les parties prenantes touchées**, qu'il s'agisse d'employés, de clients, de fournisseurs ou autres. On dit qu'il coûte cinq fois plus cher d'attirer un nouveau client que de conserver un client existant. Cela démontre l'importance de communiquer efficacement après une cyberattaque, car l'opinion de vos publics clés sera le moteur de votre capacité à maintenir la confiance dans votre organisation. Communiquez avec les publics prioritaires dès le début et au besoin lorsque de nouveaux développements surviennent. Même sans une multitude de détails, vous pouvez les informer qu'une enquête est en cours et leur fournir d'autres mises à jour à mesure que l'enquête avance.

Le pire des scénarios est de laisser vos parties prenantes être informées par les médias ou découvrir la brèche par hasard. Dès le départ, votre objectif doit être de maîtriser le canal de communication entre votre organisation et les principaux publics. Une fois ces canaux de communication établis, vous voudrez les garder à jour, ce qui vous permettra de répondre directement aux préoccupations des parties prenantes, de les tenir au courant de l'avancement

LES COMMUNICATIONS PENDANT LA PHASE DE RÉACTION À UNE CYBERATTAQUE SONT LES SUIVANTES :

- ✓ Activation de l'équipe d'intervention de crise
- ✓ Intégration d'experts en matière de cybersécurité, d'affaires juridiques, d'assurance et d'activités de l'entreprise à l'équipe d'intervention de crise
- ✓ Collaboration avec des cyberexperts pour contenir la brèche et en déterminer la portée (c'est-à-dire le type de renseignements personnels identifiables qui ont été dérobés et les personnes touchées)
- ✓ Consultation de l'équipe juridique pour la préparation des lettres de notification officielles
- ✓ Déterminer si le ou les commissaires à la protection de la vie privée ou les corps policiers doivent être informés, en fonction de la juridiction
- ✓ Conseil stratégique et planification des communications
- ✓ Suivi et gestion des enjeux
- ✓ Relations avec les employés et les parties prenantes
- ✓ Gestion des relations avec les médias
- ✓ Rédaction/révision et développement de contenus, questions-réponses et déclarations
- ✓ Surveillance des médias traditionnels et sociaux et analyse des problèmes

de l'enquête et de les informer de toute mesure prise ultérieurement. Comme les communications vont dans les deux directions, le fait de maintenir une ligne de communication ouverte vous aidera également à évaluer le niveau de soutien ou de frustration à l'égard de votre organisation et à déterminer une réponse appropriée.

Si vous êtes confronté à une attaque de type rançongiciel, cela ajoute une certaine complexité à votre réponse. En général, une attaque par rançongiciel implique que des cybercriminels accèdent à vos données, les cryptent, exigent un paiement pour rétablir l'accès à celles-ci et menacent de les diffuser sur le Web clandestin. Cela signifie que vos données sont compromises et que d'autres personnes peuvent les consulter. La prévalence et le risque des rançongiciels ne cessent de croître. Dans une enquête mondiale réalisée en 2020 par Sophos, une société de sécurité basée au Royaume-Uni, 96 % des organisations au Canada dont les données avaient été cryptées les ont récupérées, deux fois plus (56 %) grâce à des sauvegardes plutôt qu'au paiement d'une rançon (26 %). Environ 39 % des répondants au Canada (80 sur total de 200) ont été touchés par une attaque de type rançongiciel en 2020, et 68 % des entreprises canadiennes non touchées par un tel incident s'attendent à l'être à l'avenir. Il est intéressant de noter que 20 % des personnes interrogées présentent des lacunes dans leur police d'assurance en cybersécurité, ce qui signifie que les attaques par rançongiciels ne sont pas couvertes par leur assurance.

Enfin, lors de la rédaction de vos communications, ne commencez pas par le milieu de l'histoire. Dans un souci de transparence, commencez par son début. La fidélité à la marque que vous susciterez n'a pas de prix.

Reprise après une brèche de sécurité

Lorsqu'une cyberattaque est surmontée, il est important d'évaluer votre réaction à l'incident et de veiller à maintenir la confiance de vos principales parties prenantes. En évaluant leur réaction à la brèche au moyen de vérifications de la réputation ainsi que de rapports et d'analyses de renseignements sur les médias sociaux, les organisations ont la possibilité de réfléchir aux leçons tirées et d'appliquer ces connaissances à leur plan de cybersécurité et de communication de crise.

Il est important de documenter les mesures que vous avez prises pour contenir la brèche et les nouveaux processus qui seront mis en place à l'avenir. Il s'agit d'informations essentielles à partager avec vos publics clés pour démontrer que vous avez tiré des leçons de l'incident et que vous faites tout ce qui est en votre pouvoir pour éviter qu'une attaque de ce genre ne se reproduise.

Dans de nombreux cas, les entreprises proposent des services d'assistance tels que la surveillance du crédit afin de fournir des protections supplémentaires si des informations personnelles ont été compromises. Certaines entreprises fourniront une surveillance du crédit pour une période allant d'un à trois ans pour les personnes touchées, et dans le meilleur des cas, jusqu'à cinq ans.

Il est également essentiel, à la suite d'un cyberincident, d'évaluer l'efficacité de la formation sur les protocoles améliorés et de mettre en œuvre des mesures de sécurité supplémentaires (par exemple, un logiciel antivirus). Dans certains cas, cela implique de faire appel à des experts externes en cybersécurité pour réaliser une vérification et une analyse de votre infrastructure informatique et de continuer à mettre à jour les protocoles de surveillance de la sécurité et les mesures de prévention.

Finalement, il est important que les organisations réfléchissent à la façon de reconstruire leur image de marque et de conserver la confiance de leurs publics clés. Une approche judicieuse en matière de restauration de la marque et de gestion de la réputation leur permettra de transformer cette crise en une opportunité en partageant les leçons tirées de cet incident et en faisant preuve d'un leadership efficace.

LES COMMUNICATIONS PENDANT LA PHASE D'ÉVALUATION ET DE RÉCUPÉRATION COMPRENNENT :

- ✓ Analyse après l'incident et examen de la réputation
- ✓ Planification des communications pour rétablir les relations avec les parties prenantes et leur confiance
- ✓ Évaluations après l'incident : ateliers et rapport sur les « leçons tirées »
- ✓ Vérification de la réputation et plan de gestion
- ✓ Mises à jour du plan de communication en cas de crise
- ✓ Plan de gestion de la réputation et communications

Conclusion

Une chose est certaine, lorsqu'il s'agit de cyberattaques, la question n'est pas de savoir si cela se produira, mais plutôt quand cela se produira.

Avec la menace croissante et la prévalence des cyberattaques, il est essentiel que les entreprises intègrent des communications efficaces dans leur plan de crise. Si l'on ajoute à cela le risque d'une exposition plus élevée en raison de la dispersion de la main-d'œuvre et d'une surveillance réglementaire accrue, les entreprises subissent une pression énorme pour lutter contre ces menaces en temps réel.

Bien que la meilleure stratégie soit la prévention (et que de nombreuses entreprises parviennent à contrer les attaques), la fréquence et la sophistication accrues des attaques rendent de plus en plus difficile la protection de vos données dans un monde virtuel. Malgré ces enjeux, il existe des mesures que vous pouvez prendre pour protéger vos données et réagir rapidement si vous êtes victime d'une cyberattaque.

Nous espérons que ce document vous donnera quelques pistes de réflexion sur la manière dont vous pouvez vous préparer efficacement à réagir à une cyberattaque et à la surmonter. Nous serions heureux d'avoir la possibilité de passer en revue vos plans.

Références

1. **« Rapport sur la cybersécurité de 2020 de l'ACEI »**
   Autorité canadienne pour les enregistrements Internet

2. **« De nouvelles obligations en matière de déclaration des atteintes aux données entrent en vigueur cette semaine »**
   Commissariat à la protection de la vie privée du Canada
   29 octobre 2018

3. **« Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc. »**
   Rapport de conclusions
   Rapport de conclusions d'enquête en vertu de la LPRPDE no 2019-002
   25 avril 2019

4. **« Renforcer la protection de la vie privée dans l'ère numérique »**
   Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques
   Innovation, Sciences et Développement économique Canada
   21 mai 2019

5. **« Sondage auprès des Canadiens sur la protection de la vie privée de 2016 »**
   Réalisé pour le Commissariat à la protection de la vie privée du Canada par la société Phoenix SPI
   Décembre 2016

6. **« Vision du Canada pour la sécurité et la prospérité dans l'ère numérique »**
   Ministère de la Sécurité publique et de la Protection civile
   28 mai 2019

7. **« Does It Still Cost 5x More To Create A New Customer Than Retain An Old One? »**
   Blake Morgan
   Forbes Magazine - 29 avril 2019

À propos des auteurs

KAREN WHITE
chapeaute l'équipe de gestion de crises et d'enjeux de NATIONAL. Elle est l'une de nos expertes principales en matière de cybersécurité.

LARRY MARKOWITZ
est avocat et spécialiste des communications financières. Il est un membre clé de notre équipe spécialisée en communication lors d'incidents de cybersécurité.

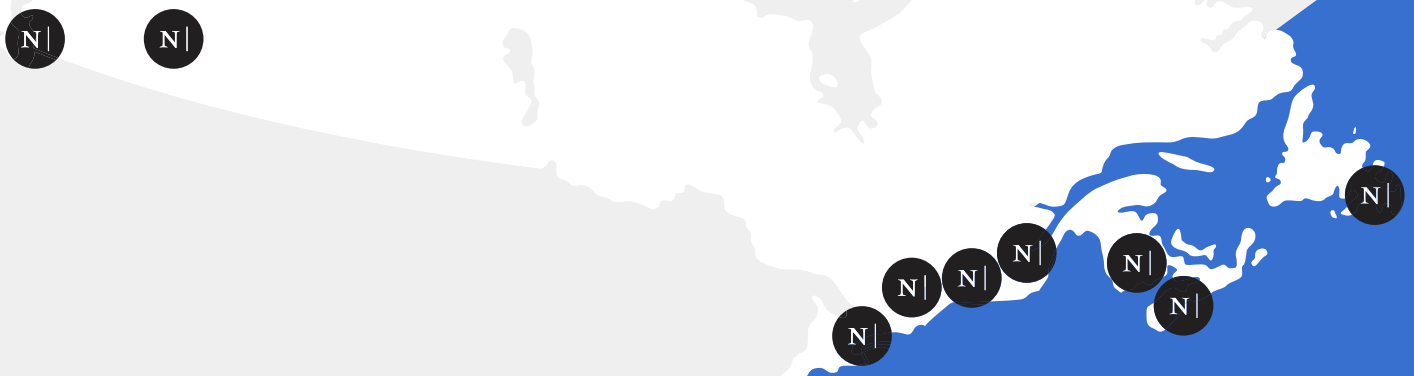
ODANE FINNEGAN
fait partie de notre équipe spécialisée en recherche sur les médias sociaux. Il est particulièrement intéressé par l'utilisation des données et de la recherche dans le cadre de stratégies de communication.

Pour en savoir plus au sujet de notre expertise en cybersécurité, visitez le **national.ca/cybersecurite**.
Contactez nos experts en cybersécurité : **cyber@national.ca**.

À propos du Cabinet de relations publiques NATIONAL

Au Cabinet de relations publiques NATIONAL, notre rôle consiste à mettre les clients en relation avec les gens qui importent, à travers les bons messages, livrés au bon moment. Grâce à la recherche, aux perspectives uniques qui en découlent et à une profonde compréhension des secteurs d'activité, nous élaborons des solutions créatives, capables de mobiliser les gens dans la réflexion et l'action. Depuis 45 ans, nous sommes au cœur d'enjeux et d'industries clés, à créer le changement pour aujourd'hui et pour demain.

NATIONAL est la plus importante firme-conseil en relations publiques au Canada, desservant des clients dans un large éventail de secteurs, avec des bureaux à Vancouver, Calgary, Toronto, Ottawa, Montréal, Québec, Saint John, Halifax et Saint-Jean. L'offre de NATIONAL inclut également NATIONAL Marchés des capitaux, chef de file de l'industrie en relations investisseurs et communication financière. Le Cabinet de relations publiques NATIONAL fait partie d'AVENIR GLOBAL, parmi les 15 plus importantes firmes de communication au monde avec des bureaux dans 23 villes au Canada, aux États-Unis, en Europe et au Moyen-Orient, et membre du Groupe conseil RES PUBLICA. À l'échelle internationale, NATIONAL est affilié à BCW, une compagnie WPP.



national.ca

N|A|T|I|O|N|A|L

national.ca